PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-095591
(43)Date of publication of application : 08.04.1994

(51)Int.Cl. G09C 1/00
G06F 12/00
H04L 9/06
H04L 9/14
H04L 12/22

(21)Application number : 04-126737
(22)Date of filing : 20.04.1992

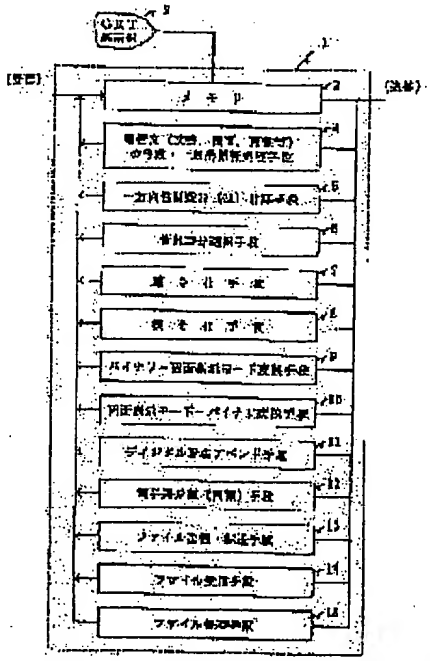
(71)Applicant : OKANO HIROICHI
(72)Inventor : OKANO HIROICHI

(30)Priority

Priority number : 03116753 Priority date : 19.04.1991 Priority country : JP
03355858 20.12.1991 JP

(54) ELECTRONIC DOCUMENT SIGNATURE AND ITS DEVICE

(57)Abstract:
PURPOSE: To enable one or more than one members to carry out digital signa ture on an electronic document (document, drawing, image, etc.) by enciphering a selected ordinary signature by way of using a secret key.
CONSTITUTION: A general information processing means 4 writes a one-way functional value, a post and a name, a document number, date and time and a message as ordinary signature. Thereafter, to make digital signature, an ordinary sentence is selected by an information partial selection means 6, and by using a secret key by enciphering means 7, the one-way functional value, the post and the name, the document number, the date and the time and the message are enciphered. By a binary display mode conversion means 9, the enciphered digital signature of binary mode is converted to display mode digital signature and it is confirmed on a display part of a screen and others. In case of receiving by a file receiving means 14, the display mode digital signature is converted to the binary digital signature by a screen display mode binary conversion means 10, the digital signature is decoded by a disclosing key by decoding means 8 and decoded to the ordinary signature.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] In the system by which one or more members perform a digital signature to an electronic filing document A general information processing means to fill in the signature of a plaintext in said electronic filing document, and an information partial selection means to choose the signature of said plaintext, The encryption means for enciphering said selected plaintext signature using a private key, and creating a digital signature, Electronic-filing-document signature equipment characterized by including a decryption means to choose said enciphered digital signature with said information partial selection means, and to decode to a plaintext signature using a public key.
[Claim 2] Electronic-filing-document signature equipment characterized by including a general information processing means to enter the signature of a plaintext in an electronic filing document as said electronic filing document at another file in the system by which one or more members perform a digital signature, the encryption means for enciphering said plaintext signature using a private key, and creating a digital signature, and a means to append said enciphered digital signature to said electronic filing document.
[Claim 3] Electronic-filing-document signature equipment characterized by including the binary display mode transformation means for displaying the digital signature of the enciphered binary mode on a display in the system by which one or more members perform a digital signature to an electronic filing document, and the display-mode-binary conversion means for changing said display-mode digital signature into a binary mode.
[Claim 4] That with which one or more members, on the other hand, express tropism function value H (M), an affiliation name, or an affiliation name to an electronic filing document as a plaintext signature in the system which performs a digital signature, a publication number, electronic-filing-document signature equipment characterized by including a general information processing means to fill in days-and-months time of day.
[Claim 5] Electronic-filing-document signature equipment characterized by including a general information processing means by which one or more members enter a message in an electronic filing document as a part of plaintext signature in the system which performs a digital signature.
[Claim 6] In the system by which a pin center,large and two or more members constitute a network in the shape of a loop formation, and circulate electronic filing documents (a document, a drawing, image, etc.) The memory which builds in a control program, and a general information processing means to draw up an electronic filing document, The display which displays an electronic filing document, and a means to, calculate tropism function H (M) on the other hand, In the electronic-filing-document signature equipment possessing a means to encipher an information part, a means to decrypt an information part, a means to transmit a file and to transmit, a file receiving means, and a file preservation means A document addresser (or pin center,large) includes following (1) thru/or the procedure of (7) in the case of transmission of a document. Each member A document addresser (or pin center,large) is the electronic-filing-document signature approach characterized by including following (15) thru/or the procedure of (19) in the case of reception of a document further including following (8) thru/or the procedure of (14).
A document addresser's (or pin center,large) document submission operation.
(1) The procedure which creates correspondence (a document, a drawing, image, etc.).
(2) On the other hand, calculate tropism function value H (M), and it is a sending agency (pin center,large) as a display mode. Procedure of writing down the calculated value in a signature part (display).
(3) Procedure of entering a sending agency affiliation name (or code), a publication number, days-and-months time of day, and a message in a sending agency (pin center,large) signature part further (display).
(4) The procedure which enciphers a display-mode H(M) dispatch former affiliation name (or code), a publication number, days-and-months time of day, and a message (plaintext signature) with a private key, and creates a binary digital signature.
(5) The procedure of changing a binary digital signature into a display-mode digital signature, and filling in a sending agency (pin center,large) signature part (display).
(6) The procedure transmitted to the next member.
(7) The procedure of saving a file.
Actuation of each member.
(8) The procedure of receiving display-mode digital office naming correspondence.
(9) The procedure which changes a display-mode digital signature into a binary digital signature, and is decoded to a plaintext signature with a public key.
(10) The procedure of checking a plaintext signature and checking H (M) being re-calculated and there being no modification in a document further.

(11) The procedure which enters H (M), an affiliation name (or code), a publication number, days-and-months time of day, and a message in the signature part of self (display), and creates a plaintext signature.
(12) A plaintext signature is enciphered with a self private key, consider as a binary digital signature, change into a display-mode digital signature further, and fill in the signature part of self (display). Or procedure to append.
(13) The procedure transmitted to the next member.
(14) The procedure of saving a file.
Document reception actuation of a document addresser (or pin center,large).
(15) The procedure of receiving display-mode digital office naming correspondence.
(16) The procedure which changes the display-mode digital signature of a sending agency (pin center,large) and all members into a binary digital signature, and is further decoded to a plaintext signature with a public key.
(17) The procedure of checking a plaintext signature of a sending agency (pin center,large) and all members, and checking H (M) being re-calculated and there being no modification in a document.
(18) The procedure of saving a file.
(19) The procedure of putting up all members' digital office naming correspondence to an electronic bulletin board (it being the multiple address to all members).
[Claim 7] In the system by which a document addresser (or pin center,large) and two or more members constitute a network in the shape of a star, and circulate electronic filing documents (a document, a drawing, image, etc.) The memory which builds in a control program, and a general information processing means to draw up an electronic filing document, In the electronic-filing-document signature equipment possessing the display which displays an electronic filing document, a means to encipher an information part, a means to decrypt an information part, a means to transmit a file and to transmit, a file receiving means, and a file preservation means A document addresser (or pin center,large) includes following (20) thru/or the procedure of (26) in the case of transmission of a document. Each member A document addresser (or pin center,large) is the electronic-filing-document signature approach characterized by including following (34) thru/or the procedure of (39) in the case of reception of a document further including following (27) thru/or the procedure of (33).
Document transmitting actuation of a document addresser (or pin center,large).
(20) The procedure which creates correspondence (a document, a drawing, image, etc.).
(21) The procedure of asking for tropism function value H (M) on the other hand, considering as a display mode, and filling in a sending agency (pin center,large) signature part from Correspondence M (display).
(22) Procedure of entering a sending agency affiliation name (or code), a publication number, days-and-months time of day, and a message in a sending agency (pin center,large) signature part further (display).
(23) The procedure which enciphers a display-mode H(M) dispatch former former affiliation name (code), a publication number, days-and-months time of day, and a message (plaintext signature) with a private key, and creates a binary digital signature.
(24) Change a binary digital signature into a display-mode digital signature, and fill in a sending agency (pin center,large) signature part (display).
(25) The procedure of putting up display-mode digital office naming correspondence to an electronic bulletin board (it being the multiple address to all members).
(26) The procedure of saving a file.
Actuation of each member.
(27) The procedure of receiving correspondence with a display-mode digital signature from a sending agency (pin center,large).
(28) Change a display-mode digital signature into a binary digital signature, and it is a pan. Procedure decoded to a plaintext signature with a public key.
(29) The procedure of checking a plaintext signature and checking H (M) being re-calculated and there being no modification in a document.
(30) The procedure which enters display-mode H (M), an affiliation name, a publication number, days-and-months time of day, and a message in the digital signature file of self (display), and creates a plaintext signature.
(31) The procedure which enciphers a plaintext signature with a self private key, makes a binary digital signature, and is further changed into a display-mode digital signature.
(32) The procedure of transmitting the display-mode digital signature of self to a pin center,large.
(33) The procedure of saving a file.
Document reception actuation of a document addresser (or pin center,large).
(34) The procedure of receiving each member's digital signature.
(35) The procedure of decoding each member's digital signature with each public key, and obtaining a plaintext signature.
(36) The procedure of checking each member's content of a signature.
(37) The procedure which adds all members' display-mode digital signature enciphered by correspondence.
(38) The procedure of saving a file.
(39) The procedure of putting up display-mode digital office naming correspondence of a document addresser (or pin center,large) and all members to an electronic bulletin board (multiple address).
[Claim 8] The electronic-filing-document signature approach and equipment claims 1 or 2 characterized by including the means which rewrites the attribute of correspondence and is considered as prohibition in the system by which one or more members perform a digital signature to an electronic filing document, 3 or 4, 5 or 6, or given in seven.
[Claim 9] Electronic-filing-document signature equipment characterized by including a printing means to print

display-mode digital office naming correspondence in a form, in the system by which one or more members perform a digital signature to an electronic filing document.

[Claim 10] Electronic-filing-document signature equipment according to claim 9 which changes a means to input the display-mode digital signature of the printed display-mode digital office naming correspondence into memory with a scanner etc. in the system by which one or more members perform a digital signature to an electronic filing document, and to display on a display, and said display-mode digital signature into a binary digital signature, and is characterized by including a decode means to decode to a plaintext signature further.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the electronic-filing-document signature approach and equipment for one or more members to perform a digital signature to electronic filing documents, such as a document, a drawing, and an image.
[0002]
[Description of the Prior Art] the conventional electronic signature — an addresser — in order to attest a principal, there is a method of sticking photograph and fingerprint of a document preparation person or a document addresser on electronic filing documents, such as a document, a drawing, and an image, etc. There is a method of specifying the addresser and addressee of a document by preparing each member's file box and next, limiting a user with a password. Furthermore, there is a digital signature method using public key encryption, such as RSA. In the so-called public key cryptosystem, an encryption key is exhibited and the decode key is made secret. Generally, an encryption key and a decode key can be replaced in a public key cryptosystem. Therefore, when using this for the signature in an electronic filing document, i.e., a digital signature, the transmitting person is attested by enciphering with the decode key of secrecy and decrypting with a open encryption key. Furthermore, in order to prevent modification of a document, on the other hand, the tropism function was used, output [of a certain short fixed length] H (M) was obtained from correspondence (M) as the function value, and the value is enciphered. There is an easy method of on the other hand adding correspondence by exclusive OR every 64 bits as a tropism function. Digital signature principle drawing is shown in drawing 7 . On the other hand, the document addresser A is a tropism function H(M) count means while sending correspondence to Addressee B. It is 100, on the other hand, asks for tropism function value H (M), and is an encryption means with a private key (decode key of a public key system). It enciphers by 101, considers as a digital signature, and transmits to the communication link place B. B receives correspondence (M) and a digital signature and is a decode means with a public key (cryptographic key of a public key system) about a digital signature. While decrypting by 102, an addresser is attested by [which asked from the correspondence which received] on the other hand being in agreement with tropism function value H (M). Correspondence can also be made into a cipher in order to perform a still safer communication link. Since only the document addresser A owns the private key, A can be specified, and it is guaranteed that there is no modification by the content of the electronic filing document by tropism function value H (M) on the other hand.
[0003]
[Problem(s) to be Solved by the Invention] however, it mentioned above — with the electronic signature approach of the time former, or equipment, there is a trouble, respectively. First, by the approach of sticking photograph and fingerprint of a document preparation person or a document addresser, it is easily forged by the electronic copy. The security according to a password with the approach of preparing each member's file box and next, limiting a user with a password is not so strong. Furthermore, by the digital signature method using the public key encryption proposed now, with correspondence, since a digital signature is sent as another file and moreover does not perform encryption/decryption on application, a problem is in a man machine interface. It is made in order that this invention may solve this trouble, and in order that one or more members may perform a digital signature to electronic filing documents (a document, a drawing, image, etc.), it aims at offering the effective electronic-filing-document signature approach and equipment.
[0004]
[Means for Solving the Problem] First, the vocabulary used first here is defined. A "digital signature" means the enciphered general electronic signature. Moreover, "a plaintext signature" is a signature of a plaintext before enciphering. A "binary digital signature" is a signature of the binary mode which enciphered the plaintext signature, and since a "display-mode digital signature" displays on a screen etc., it changes a binary digital signature into display modes, such as an ASCII code. Therefore, the "digital signature" only contains the "binary digital signature" and the "display-mode digital signature." Moreover, although an electronic filing document includes correspondence and a signature, an electronic filing document and correspondence are used without distinguishing not much. In the system by which, as for the electronic-filing-document signature equipment of claim 1 of this application, one or more members perform a digital signature to an electronic filing document A general information processing means to fill in the signature of a plaintext in said electronic filing document, and an information partial selection means to choose the signature of said plaintext, It is characterized by including the encryption means for enciphering said selected plaintext signature using a private key, and creating a digital signature, and a decryption means to choose

said enciphered digital signature with said information partial selection means, and to decode to a plaintext using a public-key.

[0005] The electronic-filing-document signature equipment of claim 2 of this application is characterized by including a general information processing means to enter the signature of a plaintext in an electronic filing document as said electronic filing document at another file in the system by which one or more members perform a digital signature, the encryption means for enciphering said plaintext signature using a private key, and creating a digital signature, and a means to append said enciphered digital signature to said electronic filing document. The electronic signature equipment of claim 3 of this application is characterized by including the binary display mode transformation means for displaying a binary digital signature on a display, and the display-mode-binary conversion means for changing the digital signature of said display mode into a binary mode in the system by which one or more members perform a digital signature to an electronic filing document. The electronic-filing-document signature equipment of claim 4 of this application is characterized by including a general information processing means to fill in that with which one or more members, on the other hand, express tropism function value H (M), an affiliation name, or an affiliation name to an electronic filing document as a digital signature in the system which performs a digital signature, a publication number, and days-and-months time of day. The electronic-filing-document signature equipment of claim 5 of this application is characterized by including a general information processing means by which one or more members enter a message in an electronic filing document as a part of plaintext signature in the system which performs a digital signature.

[0006] In the system by which a pin center,large and two or more members constitute a network in the shape of a loop formation, and the electronic-filing-document signature approach of claim 6 of this application circulates electronic filing documents (a document, a drawing, image, etc.) The memory which builds in a control program, and a general information processing means to draw up an electronic filing document, The display which displays an electronic filing document, and a means to, calculate tropism function value H (M) on the other hand, In the electronic-filing-document signature equipment possessing a means to encipher an information part, a means to decrypt, a means to transmit a file and to transmit, a file receiving means, and a file preservation means A document addresser (or pin center,large) includes following (1) thru/or the procedure of (7) in the case of transmission of a document. Each member A document addresser (or pin center,large) is further characterized by including following (15) thru/or the procedure of (19) including following (8) thru/or the procedure of (14) in the case of reception of a document.

A document addresser's (or pin center,large) document submission operation.

(1) The procedure which creates correspondence (a document, a drawing, image, etc.).

(2) On the other hand, calculate tropism function value H (M), and it is a sending agency (pin center,large) as a display mode. Procedure of writing down the calculated value in a signature part (display).

(3) Procedure of entering a sending agency affiliation name (or code), a publication number, days-and-months time of day, and a message in a sending agency (pin center,large) signature part further (display).

(4) The procedure which enciphers a display-mode H(M) dispatch former affiliation name (or code), a publication number, days-and-months time of day, and a message (plaintext signature) with a private key, and creates a binary digital signature.

(5) The procedure of changing a binary digital signature into a display-mode digital signature, and filling in a sending agency (pin center,large) signature part (display).

(6) The procedure transmitted to the next member.

(7) The procedure of saving a file.

[0007] Actuation of each member.

(8) The procedure of receiving display-mode digital office naming correspondence.

(9) The procedure which changes a display-mode digital signature into a binary digital signature, and is decoded to a plaintext signature with a public key.

(10) The procedure of checking a plaintext signature and checking H (M) being re-calculated and there being no modification in a document further.

(11) The procedure which enters H (M), an affiliation name (or code), a publication number, days-and-months time of day, and a message in the signature part of self (display), and creates a plaintext signature.

(12) A plaintext signature is enciphered with a self private key, consider as a binary digital signature, change into a display-mode digital signature further, and fill in the signature part of self (display). Or procedure to append.

(13) The procedure transmitted to the next member.

(14) The procedure of saving a file.

Document reception actuation of a document addresser (or pin center,large).

(15) The procedure of receiving display-mode digital office naming correspondence.

(16) The procedure which changes the display-mode digital signature of a sending agency (pin center,large) and all members into a binary digital signature, and is decoded to a plaintext signature with a public key.

(17) The procedure of checking a plaintext signature of a sending agency (pin center,large) and all members, and checking H (M) being re-calculated and there being no modification in a document.

(18) The procedure of saving a file.

(19) The procedure of putting up all members' digital office naming correspondence to an electronic bulletin board (it being the multiple address to all members).

[0008] In the system by which two or more members constitute a network in the shape of a star with a document

addresser (or pin center,large), and the electronic-filing-document signature approach of claim 7 of this application circulates electronic filing documents (a document, a drawing, image, etc.) The memory which builds in a control program, and an information processing means to create correspondence, i.e., an electronic filing document, In the electronic-filing-document signature equipment possessing the display which displays an electronic filing document, a means to transmit a file and to transmit, a file receiving means, and a file preservation means A document addresser (or pin center,large) includes following (20) thru/or the procedure of (26) in the case of transmission of a document. Each member A document addresser (or pin center,large) is further characterized by including following (34) thru/or the procedure of (39) including following (27) thru/or the procedure of (33) in the case of reception of a document.

Document transmitting actuation of a document addresser (or pin center,large).

(20) The procedure which creates correspondence (a document, a drawing, image, etc.).

(21) The procedure of asking for tropism function value H (M) on the other hand, considering as a display mode, and filling in a sending agency (pin center,large) signature part from Correspondence M (display).

(22) Procedure of entering a sending agency affiliation name (or code), a publication number, days-and-months time of day, and a message in a sending agency (pin center,large) signature part further (display).

(23) The procedure which enciphers a display-mode H(M) dispatch former former affiliation name (code), a publication number, days-and-months time of day, and a message (plaintext signature) with a private key, and creates a binary digital signature.

[0009] (24) Change a binary digital signature into a display-mode digital signature, and fill in a sending agency (pin center,large) signature part (display).

(25) The procedure of putting up display-mode digital office naming correspondence to an electronic bulletin board (it being the multiple address to all members).

(26) The procedure of saving a file.

Actuation of each member.

(27) The procedure of receiving correspondence with a display-mode digital signature from a sending agency (pin center,large).

(28) The procedure which changes a display-mode digital signature into a binary digital signature, and is decoded with a public key.

(29) The procedure of checking a plaintext signature and checking H (M) being re-calculated and there being no modification in a document.

(30) The procedure which enters display-mode H (M), an affiliation name, a publication number, days-and-months time of day, and a message in the digital signature file of self (display), and creates a plaintext signature.

(31) The procedure which enciphers a plaintext signature with a self private key, makes a binary digital signature, and is further changed into a display-mode digital signature.

(32) The procedure of transmitting the display-mode digital signature of self to a pin center,large.

(33) The procedure of saving a file.

[0010] Document reception actuation of a document addresser (or pin center,large).

(34) The procedure of receiving each member's digital signature.

(35) The procedure of decoding each member's digital signature with each public key, and obtaining a plaintext signature.

(36) The procedure of checking each member's content of a signature.

(37) The procedure which adds all members' display-mode digital signature enciphered by correspondence.

(38) The procedure of saving a file.

(39) The procedure of putting up display-mode digital office naming correspondence of a document addresser (or pin center,large) and all members to an electronic bulletin board (multiple address).

[0011] The electronic-filing-document signature equipment of claim 8 of this application is characterized by including the means which rewrites the attribute of correspondence and is considered as prohibition in the system by which one or more members perform a digital signature to an electronic filing document. The electronic-filing-document signature equipment of claim 9 of this application is characterized by including a printing means to print display-mode digital office naming correspondence in a form in the system by which one or more members perform a digital signature to an electronic filing document. The electronic-filing-document signature equipment of claim 10 of this application is characterized by including a decryption means to decode to a plaintext signature further in the system by which one or more members perform a digital signature to an electronic filing document by changing a means to input the display-mode digital signature of the printed display-mode digital office naming correspondence into memory with a scanner etc., and to display on a display, and said display-mode digital signature into a binary digital signature.

[0012]

[Function] According to the electronic-filing-document signature approach and equipment of this application, as a plaintext signature of self, while being calculated from correspondence, tropism function value H (M), an affiliation name (code), a publication number, days-and-months time of day, and a message are written in, and it enciphers with a private key, and the system by which one or more members perform a digital signature to an electronic filing document is filled in as a digital signature. The enciphered binary digital signature is changed into a display-mode digital signature. Moreover, all members' digital signature is decrypted with a public key, it checks that tropism function value H (M) is re-calculated on the other hand, and there is no modification in a document, and an affiliation

name, a publication number, days-and-months time of day, and a message are inspected. Moreover, digital office naming correspondence is displayed on an electronic bulletin board, and the multiple address is carried out to all members.

[0013]

[Example] the fundamental way of thinking of this invention is ** as application ****** at an electronic filing document as as it is as possible about authentication with the seal of the document on forms, such as a circulation document currently performed actually or a charter. This invention is explained in full detail based on the drawing in which the example is shown below. Drawing 1 is a block diagram showing the functional configuration of the electronic-filing-document signature equipment concerning one example of this invention. Drawing 2 is a flow chart which shows actuation of this electronic-filing-document signature equipment when constituting a loop-formation-like network, and drawing 3 is the correspondence and example of a digital signature. Drawing 4 is a flow chart which shows actuation of this electronic-filing-document signature equipment when constituting a star-like network, and drawing 5 is the correspondence and example of a digital signature.

[0014] Drawing 1 is a block diagram showing the functional configuration of the electronic-filing-document signature equipment with which one or more members provide electronic filing documents (a document, a drawing, image, etc.) with an effective digital signature in the system which performs a digital signature. First, control section 1 consists of a microprocessor and is memory. Data processing later mentioned with the control program currently written in 3 is performed. It explains supposing the virtual block diagram which has this processing facility below. General information processing means 4 draws up an electronic filing document and is a display about it. It displays on 2. Subsequently, on the other hand, it is a tropism function H(M) count means. On the other hand, 5 calculates tropism function value H (M) from correspondence (M). General information processing means 4 writes in H (M), an affiliation name, a publication number, days-and-months time of day, and a message as a signature of a plaintext. Next, it is an information partial selection means in order to create a digital signature. A plaintext is chosen by 6 and it is an encryption means. By 7, H (M), an affiliation name, a publication number, days-and-months time of day, and a message are enciphered using private keys (decode key of a public key system etc.). And binary display-mode conversion means By 9, the digital signature as which the binary mode was enciphered is changed into a display-mode digital signature, and it checks on displays, such as a screen. A means to file-transmit and to transmit next A file is transmitted and transmitted by 13 and it is a file preservation means. A file is saved by 15. File receiving means When an electronic filing document is received by 14, it is a screen-display mode-binary conversion means. By 10, a display-mode digital signature is changed into a binary digital signature, a digital signature is decoded with a public key (a public key system cryptographic key) with the decryption means 8, H (M) is re-calculated, and the content of a signature is checked. A means to notify an electronic bulletin board in the pin center,large Correspondence and all members' digital signature are put up for an electronic bulletin board by 12 (multiple address). Digital signature appending means 11 appends a digital signature to correspondence. In addition, in case a plaintext signature is created, in order to carry out a screen display, on the other hand, it is a binary display-mode conversion means about tropism function value H (M). It changes into a display mode by 9. Since explanation becomes complicated, below, this processing about H (M) is omitted.

[0015] In case invention described below is carried out, only a required thing is used among the functional means of drawing 1. Moreover, in the following explanation and a drawing, "the display" is only used in the same semantics with a "screen display", and "a display for various display means including a screen" is meant. It sets to the system by which one or more members perform a digital signature to an electronic filing document, and the electronic-filing-document signature equipment of claim 1 of this application is a general information processing means. By 4, a plaintext signature is filled in in an electronic filing document, and it is an information partial selection means. A plaintext signature is chosen by 6. A private key is used for the selected plaintext signature, and it is an encryption means. It enciphers by 7 and a digital signature is created. The enciphered digital signature is an information partial selection means. It is chosen by 6, a public key is used and it is a decryption means. 8 decodes at a plaintext signature. For the electronic-filing-document signature equipment of claim 2 of this application, it sets to the system by which one or more members perform a digital signature to an electronic filing document, and an electronic filing document is a general information processing means to another file. A plaintext signature is filled in by 4, a private key is used for the plaintext signature, and it is an encryption means. It enciphers by 7 and a digital signature is created. The enciphered digital signature is a digital signature appending means. It is 11 and is appended to an electronic filing document.

[0016] It sets to the system by which one or more members perform a digital signature to an electronic filing document, and the electronic signature equipment of claim 3 of this application is a binary display-mode conversion means about a binary digital signature, By 9, in order to display on displays, such as a screen, it changes into a display-mode digital signature. Moreover, display-mode-binary conversion means 10 changes a display-mode digital signature into a binary digital signature. It sets to the system by which one or more members perform a digital signature to an electronic filing document, and the electronic-filing-document signature equipment of claim 4 of this application is a general information processing means. 4 fills in what, on the other hand, expresses tropism function value H (M), an affiliation name, or an affiliation name as a digital signature, a publication number, and days-and-months time of day. It sets to the system by which one or more members perform a digital signature to an electronic filing document, and the electronic-filing-document signature equipment of claim 5 of this application is a general information processing means. 4 fills in a message as a part of plaintext signature.

[0017] Next, a more concrete example is shown. Now, theoretically, although there are various things in a network

configuration, as shown in the example of logical construction of drawing 6 network, it is divided into (a) loop-formation=like network configuration and (b) star-like network configuration. Below, the example of the electronic-filing-document signature equipment of drawing 1 in each network of operation is explained based on drawing 2, drawing 3, drawing 4, and drawing 5. In addition, N1, N2, and ... show procedure (step) during explanation of the flow chart shown in drawing 2 and drawing 4. The example of the electronic-filing-document signature approach of claim 6 of this application is explained in full detail. As shown in drawing 6 (a), a pin center,large and two or more members constitute a network in the shape of a loop formation, and describe the actuation in the system which circulates electronic filing documents (a document, a drawing, image, etc.) using drawing 2 and drawing 3. Although dispatch of a member to a document is possible, suppose that the document was now sent from the pin center,large.

[0018] Document transmitting actuation of a pin center,large is as follows according to drawing 2 (a). It is a general information processing means at N1. Correspondence (a document, a drawing, image, etc.) is created by 4, and, on the other hand, it is a tropism function H(M) count means at N2. On the other hand, tropism function value H (M) is calculated by 5, and it is a binary display-mode conversion means. By 9, it is made a display mode and the calculated value is written down in a sending agency (pin center,large) signature part (display). It is a general information processing means at N3. By 4, a sending agency affiliation name (code), a publication number, days-and-months time of day, and a message are filled in (display). It is an encryption means with a private key at N4 about a display-mode H(M) dispatch former affiliation name (code), a publication number, days-and-months time of day, and a message (plaintext signature). It enciphers by 7 and a binary digital signature is created. It is a binary display-mode conversion means at N5. By 9, a binary digital signature is changed into a display-mode digital signature, and a sending agency (pin center,large) signature part is filled in (display). And they are file transmission and a transfer means at N6. By 13, it transmits to the next member. It is a file preservation means at N7. A file is saved by 15.

[0019] Next, actuation of each member becomes as it is shown in drawing 2 (b). It is a file receiving means at N8. 14 receives screen-display mode digital office naming correspondence. It is a display-mode-binary conversion means at N9. Screen-display mode digital is changed into a binary digital signature by 10, and it is a decryption means. By 8, a binary digital signature is decoded with a public key (a public key system cryptographic key). A plaintext signature is checked by N10 and, on the other hand, it is a tropism function H(M) count means. H (M) is re-calculated by 5 and it checks that there is no modification in a document. It is a general information processing means at N11. By 4, H (M), an affiliation name (code), a publication number, days-and-months time of day, and a message are entered in the signature part of self (display), and a plaintext signature is created. Furthermore, it is an encryption means at N12. By 7, a plaintext signature is enciphered with private keys (decode key of a public key system etc.), and the binary digital signature of self is created. And binary display-mode conversion means It changes into a screen-display digital signature by 9, and they are entry (display) or a digital signature appending means to the signature part of self. A digital signature is appended to an electronic filing document by 11. A means to file-transmit and to transmit by N13 by 13, it transmits to the next member. It is a file preservation means at N14. A file is saved by 15.

[0020] Document reception actuation of a pin center,large becomes as it is shown in drawing 2 (c). It is a file receiving means at N15. 14 receives correspondence. It is a display-mode-binary conversion means at N16 about the display-mode digital signature of a sending agency (pin center,large) and all members. It changes into a binary digital signature by 10, and is a decryption means. By 8, the signature of self [the public key (a public key system cryptographic key) of a sending agency (pin center,large)] is decoded to a plaintext signature. A plaintext signature of a sending agency (pin center,large) and all members is checked by N17, and, on the other hand, it is a tropism function H(M) count means. By 5, H (M) is re-calculated and it checks that there is no modification in a document. It is a file preservation means at N18. A file is saved by 15. A means to put up the display-mode digital office naming correspondence of a pin center,large and all members for an electronic bulletin board if required of N19 An electronic bulletin board is notified by 11, or the multiple address is carried out to all members.

[0021] An example of the correspondence created by this electronic-filing-document signature equipment when constituting a loop-formation-like network and a digital signature is shown in drawing 3. Correspondence with a plaintext signature It is correspondence in 20. 21 and the digital signature column 22 is prepared. A pin center,large and a member enter a plaintext signature in the signature column. Since a pause notation which is different to each member's signature column, respectively as shown in drawing is used, by it, a signature part is chosen and a partial code and partial decode are performed by each cryptographic key. Instead of a pause notation, the signature column may be expressed with a coordinate or a variable, and the partial code of the signature column may be carried out based on it. Display-mode digital office naming correspondence 30 is correspondence. 31 and display-mode digital signature It consists of 32. In addition, signers who should circulate, such as a person and a contractor, are entered in correspondence, or the signature column is prepared. The example of the electronic-filing-document signature approach of claim 7 of this application is explained in full detail. As shown in drawing 6 (b), a pin center,large and two or more members constitute a network in the shape of a star, and describe the actuation in the system which circulates electronic filing documents (a document, a drawing, image, etc.) using drawing 4 and drawing 5. a pin center,large — a document — an electronic bulletin board — a bulletin — or the multiple address is carried out and each member transmits only a digital signature to a pin center,large. In addition, since the relation with the functional block diagram of drawing 1 is the same as that of the case of a loop-formation-like network, it omits in the following explanation.

[0022] First, document transmitting actuation of a pin center,large is as follows according to drawing 4 (a). Correspondence (a document, a drawing, image, etc.) is created by N20. On the other hand, tropism function value H (M) is calculated by N21, it considers as screen-display mode, and the calculated value is written down in a sending

agency (pin center,large) signature part (display). A sending agency affiliation name (code), a publication number, days-and-months time of day, and a message are entered in a sending agency (pin center,large) signature part by N22 (display). By N23, a screen-display mode H(M) dispatch former affiliation name (code), a publication number, days-and-months time of day, and a message (plaintext signature) are enciphered with a private key, and a binary digital signature is created. A binary digital signature is changed into a screen-display mode digital signature by N24, and a sending agency (pin center,large) signature part is filled in (display). By N25, the multiple address of the screen-display mode digital office naming correspondence is carried out to an electronic bulletin board to a bulletin or all members. (If required, an access privilege will be assigned to a member.) A file is saved by N26.

[0023] Actuation of each member becomes as it is shown in drawing 4 (b). Display-mode digital office naming correspondence reception is carried out from a sending agency (pin center,large) by N27, a display-mode digital signature is changed into a binary digital signature by N28, and it decodes to a plaintext signature with a public key. N29 A plaintext signature is checked and it checks that H (M) is re-calculated and there is no modification in a document. Display-mode H (M), an affiliation name (code), a publication number, days-and-months time of day, and a message are entered in the digital signature file of self [N30], and a plaintext signature is created. By N31, a plaintext signature is enciphered with a self private key, and it considers as a binary digital signature, and changes into a display-mode digital signature further. The display-mode digital signature of self [N32] is transmitted to a pin center,large. A file is saved by N33. Document reception actuation of a pin center,large becomes as it is shown in drawing 4 (c). Each member's display-mode digital signature is received by N34. Each member's display-mode digital signature is changed into a binary digital signature by N35, further, it decodes with each public key and a plaintext signature is obtained. The content of the signature of each member is checked by N36. All members' display-mode digital signature enciphered by correspondence by N37 is added. A file is saved by N38. If required of N39, display-mode digital office naming correspondence of a pin center,large and all members will be put up for an electronic bulletin board (it is the multiple address to all members).

[0024] An example of the correspondence created by this electronic-filing-document signature equipment when constituting a loop-formation-like network and a digital signature is shown in drawing 5. Display-mode digital office naming correspondence 50 is put up for an electronic bulletin board (multiple address). Correspondence 51 and the display-mode digital signature column It consists of 52. Each member is the display-mode digital signature of self. 53 and 54 are sent to a pin center,large. In the pin center,large, all members' display-mode digital signature is added to the original electronic filing document, and an electronic bulletin board is notified again (multiple address). In addition, invention of claim 8 is the electronic-filing-document signature approach and equipment which rewrite the attribute of correspondence, consider as prohibition and make the content of the digital signature an affiliation name (code), a publication number, days-and-months time of day, and a message not using tropism function value H (M) on the other hand. Since it can carry out easily from the above-mentioned explanation, this invention is omitted for details. Moreover, invention of claim 9 is the electronic-filing-document signature approach and equipment which print correspondence and a display-mode digital signature in a form, call in a part for delivery and the cryptopart on memory and a display with a manual entry, a scanner, etc., and decode it with a decode means to preservation or the others. The digital signature on a form can be treated like the usual seal. Since this can also be easily carried out from the above-mentioned explanation, it omits for details. In addition, the part which is not displayed is made when [that] a binary digital signature may be displayed on a display. Moreover, conversion of a line feed code etc. needs to be processed for turbulence of a screen. Moreover, like [in invention of claim 7], the approach of changing into a binary digital signature is also effective at the time of transmission without a member's sending a display-mode digital signature to a pin center,large. It does not pass over the example of this invention stated above to a mere example, and it does not limit this invention. Various variations occur and they also belong to this invention.

[0025]

[Effect of the Invention] As explained above, as for the electronic-filing-document signature approach and equipment of this invention, it is possible for one or more members to choose a signature part as an electronic filing document, and to make a digital signature it like seal, using the cryptographic key of secrecy. And the digital signature system excellent in the man machine interface is realizable using a display-mode digital signature.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the functional configuration of the electronic-filing-document signature equipment concerning one example of this invention.
[Drawing 2] It is the flow chart which shows actuation of this electronic-filing-document signature equipment when constituting a loop-formation-like network. For the document dispatch flow chart of pin center,large equipment, and (b), the flow chart of member equipment and (c) are [(a)] the document receiving flow chart of pin center,large equipment.
[Drawing 3] The correspondence and the digital signature which are created by this electronic-filing-document signature equipment when constituting a loop-formation-like network.
[Drawing 4] It is the flow chart which shows actuation of this electronic-filing-document signature equipment when constituting a star-like network. For the document dispatch flow chart of pin center,large equipment, and (b), the flow chart of member equipment and (c) are [(a)] the document receiving flow chart of pin center,large equipment.
[Drawing 5] It is the correspondence and the digital signature which are created by this electronic-filing-document signature equipment when constituting a star-like network.
[Drawing 6] It is a network example of logical construction. (a) is loop-formation-like network configuration and (b) is star-like network configuration.
[Drawing 7] It is digital signature principle drawing.
[Description of Notations]
1 Control Section
2 Display
3 Memory
4 General Information Processing Means
5 On the Other Hand, it is Tropism Function H(M) Count Means.
6 Information Partial Selection Means
7 Encryption Means
8 Decryption Means
9 Binary Display-Mode Conversion Means
10 Display-Mode-Binary Conversion Means
11 Digital Signature Appending Means
12 Electronic Bulletin Board (Multiple Address) Means
13 File Transmission / Transfer Means
14 File Receiving Means
15 File Preservation Means
20 Correspondence with Plaintext Signature
21 Correspondence
22 Plaintext Signature
30 Display-Mode Digital Office Naming Correspondence
31 Correspondence
32 Display-Mode Digital Signature
50 Display-Mode Digital Office Naming Correspondence
51 Correspondence
52 Display-Mode Digital Signature
53 Display-Mode Digital Signature
54 Display-Mode Digital Signature
100 On the Other Hand, it is Tropism Function H(M) Count Means.
101 Encryption Means
102 Decryption Means

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平6－95591

(43)公開日　平成6年(1994)4月8日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ　1/00		8837－5L			
Ｇ０６Ｆ　12/00	５３７　Ｈ	8526－5B			
Ｈ０４Ｌ　9/06					
		7117－5K	Ｈ０４Ｌ　9/02	Ｚ	
		8732－5K	11/26		

審査請求　未請求　請求項の数10(全 29 頁)　最終頁に続く

(21)出願番号　特願平4－126737

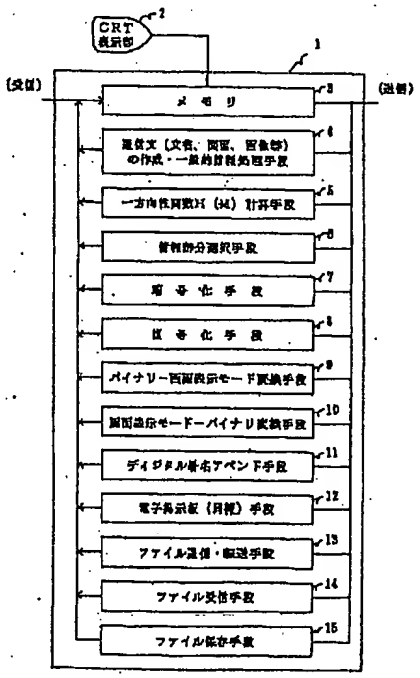
(22)出願日　平成4年(1992)4月20日

(31)優先権主張番号　特願平3－116753
(32)優先日　平3(1991)4月19日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平3－355858
(32)優先日　平3(1991)12月20日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　591059364
岡野　博一
広島県広島市安佐北区倉掛１丁目８－６
(72)発明者　岡野　博一
広島県広島市安佐北区倉掛１丁目８－６

(54)【発明の名称】　電子文書署名方法および装置

(57)【要約】
【目的】　本発明の目的は、文書、図面、画像などの電子文書に、１名以上のメンバーがディジタル署名を行うために、情報処理を行う機能に加えて、暗号機能および一方向性関数計算機能および情報部分選択機能等を有し、メンバーが自己の署名位置に、一方向性関数値、所属氏名（コード）、文書番号、月日時刻、メッセージを書き込み、自己の秘密鍵で暗号化し、さらに、表示モードディジタル署名に変換して記入（表示）し、また、受信者は公開鍵で復号して、署名を確認することができるマン・マシン・インタフェースに優れた電子文書署名方法および装置を提供することである。
【構成】電子文書（文書、図面、画像）処理システムに、暗号化機能および一方向性関数計算機能および情報部分選択手段およびバイナリー表示モード変換手段等を付加する。



1

【特許請求の範囲】

【請求項1】　電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、前記電子文書内に平文の署名を記入する一般的情報処理手段と、前記平文の署名を選択する情報部分選択手段と、選択された前記平文署名を秘密鍵を用いて暗号化しディジタル署名を作成するための暗号化手段と、前記暗号化されたディジタル署名を前記情報部分選択手段によって選択し、公開鍵を用いて平文署名に復号する復号化手段とを含むことを特徴とする電子文書署名装置。

【請求項2】　電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、前記電子文書とは別ファイルに平文の署名を記入する一般的情報処理手段と、前記平文署名を秘密鍵を用いて暗号化しディジタル署名を作成するための暗号化手段と、前記暗号化されたディジタル署名を前記電子文書にアペンドする手段とを含むことを特徴とする電子文書署名装置。

【請求項3】　電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、暗号化されたバイナリモードのディジタル署名を表示部に表示するためのバイナリー表示モード変換手段と、前記表示モードディジタル署名をバイナリモードに変換するための表示モードーバイナリ変換手段とを含むことを特徴とする電子文書署名装置。

【請求項4】　電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、平文署名として一方向性関数値H（M）、所属氏名または所属氏名を表すもの、文書番号、月日時刻を記入する一般的情報処理手段を含むことを特徴とする電子文書署名装置。

【請求項5】　電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、平文署名の一部としてメッセージを記入する一般的情報処理手段を含むことを特徴とする電子文書署名装置。

【請求項6】　センターと複数のメンバーがループ状にネットワークを構成して、電子文書（文書、図面、画像等）を回覧するシステムにおいて、制御プログラムを内蔵するメモリと、電子文書を作成する一般的情報処理手段と、電子文書を表示する表示部と、一方向性関数H（M）を計算する手段と、情報部分を暗号化する手段と、情報部分を復号化する手段と、ファイルを送信、転送する手段と、ファイル受信手段と、ファイル保存手段とを具備する電子文書署名装置において、文書発信者（あるいはセンター）は文書の送信の際には下記（1）ないし（7）の手順を含み、各メンバーは、下記（8）ないし（14）の手順を含み、さらに、文書発信者（あるいはセンター）は文書の受信の際には下記（15）ないし（19）の手順を含むことを特徴とする電子文書署名方法。

文書発信者（あるいはセンター）の文書発信操作。

（1）通信文（文書、図面、画像等）を作成する手順。

2

（2）一方向性関数値H（M）を計算し、表示モードとして、発信元（センター）　　署名箇所にその計算値を記入（表示）する手順。

（3）さらに、発信元（センター）署名箇所に、発信元所属氏名（あるいはコード）、文書番号、月日時刻、メッセージを記入（表示）する手順。

（4）表示モードH（M）、発信元所属氏名（あるいはコード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化してバイナリディジタル署名を作成する手順。

（5）バイナリディジタル署名を表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する手順。

（6）次のメンバーへ転送する手順。

（7）ファイルを保存する手順。

各メンバーの操作。

（8）表示モードディジタル署名付通信文を受信する手順。

（9）表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する手順。

（10）平文署名を確認し、さらに、H（M）を再計算して文書に変更の無いことを確認する手順。

（11）自己の署名箇所にH（M）、所属氏名（あるいはコード）、文書番号、月日時刻、メッセージを記入（表示）し、平文署名を作成する手順。

（12）自己の秘密鍵で平文署名を暗号化して、バイナリディジタル署名とし、さらに表示モードディジタル署名に変換して自己の署名箇所に記入（表示）　　あるいはアペンドする手順。

（13）次のメンバーに転送する手順。

（14）ファイルを保存する手順。

文書発信者（あるいはセンター）の文書受信操作。

（15）表示モードディジタル署名付通信文を受信する手順。

（16）発信元（センター）および全メンバーの表示モードディジタル署名をバイナリディジタル署名に変換し、さらに、公開鍵で平文署名に復号する手順。

（17）発信元（センター）および全メンバーの平文署名を確認し、H（M）を再計算し、文書に変更のないことを確認する手順。

（18）ファイルを保存する手順。

（19）全メンバーのディジタル署名付通信文を電子掲示板へ掲示（全メンバーに同報）する手順。

【請求項7】　文書発信者（あるいはセンター）と複数のメンバーがスター状にネットワークを構成して、電子文書（文書、図面、画像等）を回覧するシステムにおいて、制御プログラムを内蔵するメモリと、電子文書を作成する一般的情報処理手段と、電子文書を表示する表示部と、情報部分を暗号化する手段と、情報部分を復号化する手段と、ファイルを送信、転送する手段と、ファイ

ル受信手段と、ファイル保存手段とを具備する電子文書署名装置において、文書発信者（あるいはセンター）は文書の送信の際には下記（２０）ないし（２６）の手順を含み、各メンバーは、下記（２７）ないし（３３）の手順を含み、さらに、文書発信者（あるいはセンター）は文書の受信の際には下記（３４）ないし（３９）の手順とを含むことを特徴とする電子文書署名方法。

文書発信者（あるいはセンター）の文書送信操作。

（２０）通信文（文書、図面、画像等）を作成する手順。

（２１）通信文Mより一方向性関数値H（M）を求め、表示モードとし、発信元（センター）署名箇所に、記入（表示）する手順。

（２２）さらに、発信元（センター）署名箇所に、発信元所属氏名（あるいはコード）、文書番号、月日時刻、メッセージを記入（表示）する手順。

（２３）表示モードH（M）、発信元元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化して、バイナリディジタル署名を作成する手順。

（２４）バイナリディジタル署名を表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する。

（２５）表示モードディジタル署名付通信文を電子掲示板へ掲示（全メンバーへ同報）する手順。

（２６）ファイルを保存する手順。

各メンバーの操作。

（２７）発信元（センター）より表示モードディジタル署名付き通信文を受信する手順。

（２８）表示モードディジタル署名をバイナリディジタル署名に変換し、さらに、　　公開鍵で平文署名に復号する手順。

（２９）平文署名を確認し、H（M）を再計算して文書に変更の無いことを確認する手順。

（３０）自己のディジタル署名ファイルに表示モードH（M）、所属氏名、文書番号、月日時刻、メッセージを記入（表示）して平文署名を作成する手順。

（３１）自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに、表示モードディジタル署名に変換する手順。

（３２）自己の表示モードディジタル署名をセンターに送信する手順。

（３３）ファイルを保存する手順。

文書発信者（あるいはセンター）の文書受信操作。

（３４）各メンバーのディジタル署名を受信する手順。

（３５）各メンバーのディジタル署名をそれぞれの公開鍵で復号して平文署名を得る手順。

（３６）各メンバーの署名内容を確認する手順。

（３７）通信文に暗号化された全メンバーの表示モードディジタル署名を付加する手順。

（３８）ファイルを保存する手順。

（３９）文書発信者（あるいはセンター）と全メンバーの表示モードディジタル署名付通信文を電子掲示板へ掲示（同報）する手順。

【請求項８】　電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、通信文の属性を書換え禁止とする手段を含むことを特徴とする請求項１または２または３または４または５または６または７記載の電子文書署名方法および装置。

【請求項９】　電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、表示モードディジタル署名付通信文を用紙に印刷する印刷手段を含むことを特徴とする電子文書署名装置。

【請求項１０】　電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、印刷された表示モードディジタル署名付通信文の表示モードディジタル署名をスキャナなどでメモリに入力し、表示部上に表示する手段と、前記表示モードディジタル署名をバイナリディジタル署名に変換し、さらに、平文署名に復号する復号手段とを含むことを特徴とする請求項９記載の電子文書署名装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、文書、図面、画像等の電子文書に１名以上のメンバーがディジタル署名を行うための電子文書署名方法および装置に関する。

【０００２】

【従来の技術】従来の電子署名では、発信者本人を認証するために、文書、図面、画像等の電子文書に文書作成者あるいは文書発信者の写真および指紋を貼り付ける方法などがある。つぎに、各メンバーのファイル・ボックスを用意し、パスワードによって使用者を限定することによって、文書の発信者・受信者を特定する方法がある。さらに、ＲＳＡなどの公開鍵暗号を用いるディジタル署名方式がある。いわゆる公開鍵暗号方式においては、暗号化鍵を公開し復号鍵を非公開としている。一般的には、公開鍵暗号方式では、暗号化鍵と復号鍵を入れ替え可能である。したがって、これを電子文書における署名、すなわちディジタル署名に用いる場合、秘密の復号鍵で暗号化し、公開の暗号化鍵で復号化することによって、送信者を認証している。さらに、文書の変更を防ぐために、一方向性関数を用いて、通信文（M）からその関数値として、短いある一定長の出力H（M）を得て、その値を暗号化している。簡単な一方向性関数としては通信文を６４ビットごとに排他論理和で足し込む方法がある。図７にディジタル署名原理図を示す。文書発信者Ａは通信文を受信者Ｂに送るとともに、一方向性関数H（M）計算手段 100で、一方向性関数値H（M）を求め、秘密鍵（公開鍵方式の復号鍵）で暗号化手段 101で暗号化してディジタル署名とし、通信先Ｂへ伝送す

5

る。Ｂは通信文（Ｍ）とディジタル署名を受信し、ディジタル署名を公開鍵（公開鍵方式の暗号鍵）で復号手段102によって復号化するとともに、受信した通信文から求めた一方向性関数値Ｈ（Ｍ）と一致することによって、発信者を認証する。さらに安全な通信を行うために、通信文も暗号文とすることができる。秘密鍵は文書発信者Ａしか所有していないのでＡを特定でき、一方向性関数値Ｈ（Ｍ）によって、電子文書の内容に変更のないことが保証される。

【０００３】

【発明が解決しようとする課題】ところが、上述したごとき従来の電子署名方法または装置では、それぞれ問題点がある。まず、文書作成者あるいは文書発信者の写真および指紋を貼り付ける方法では、電子的なコピーによって容易に偽造される。つぎに、各メンバーのファイル・ボックスを用意し、パスワードによって使用者を限定する方法では、パスワードによるセキュリティはそれほど強くない。さらに、現在提案されている公開鍵暗号を用いるディジタル署名方式では、ディジタル署名は通信文とは別ファイルとして送られ、しかも、アプリケーション上では暗号化／復号化を行わないので、マンマシン・インタフェイスに問題がある。本発明はかかる問題点を解決するためになされたものであって、電子文書（文書、図面、画像等）に１名以上のメンバーがディジタル署名を行うために有効な電子文書署名方法および装置を提供することを目的とする。

【０００４】

【課題を解決するための手段】まず、最初にここで用いる用語を定義しておく。「ディジタル署名」は一般的な暗号化された電子署名を意味する。また、「平文署名」は暗号化する前の、平文の署名である。「バイナリディジタル署名」は平文署名を暗号化したバイナリモードの署名であり、「表示モードディジタル署名」は画面などに表示するために、バイナリディジタル署名をアスキーコード等の表示モードに変換したものである。したがって、単に、「ディジタル署名」は「バイナリディジタル署名」と「表示モードディジタル署名」を含んでいる。また、電子文書は通信文と署名を含むが、電子文書と通信文はあまり区別しないで用いている。本願の請求項１の電子文書署名装置は、電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、前記電子文書内に平文の署名を記入する一般的情報処理手段と、前記平文の署名を選択する情報部分選択手段と、選択された前記平文署名を秘密鍵を用いて暗号化しディジタル署名を作成するための暗号化手段と、前記暗号化されたディジタル署名を前記情報部分選択手段によって選択し、公開鍵を用いて平文に復号する復号化手段とを含むことを特徴とする。

【０００５】本願の請求項２の電子文書署名装置は、電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、前記電子文書とは別ファイルに平文の署名を記入する一般的情報処理手段と、前記平文署名を秘密鍵を用いて暗号化しディジタル署名を作成するための暗号化手段と、前記暗号化されたディジタル署名を前記電子文書にアペンドする手段とを含むことを特徴とする。本願の請求項３の電子署名装置は、電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、バイナリディジタル署名を表示部に表示するためのバイナリー表示モード変換手段と、前記表示モードのディジタル署名をバイナリモードに変換するための表示モードーバイナリ変換手段とを含むことを特徴とする。本願の請求項４の電子文書署名装置は、電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、ディジタル署名として一方向性関数値Ｈ（Ｍ）、所属氏名または所属氏名を表すもの、文書番号、月日時刻を記入する一般的情報処理手段を含むことを特徴とする。本願の請求項５の電子文書署名装置は、電子文書に１名以上のメンバーがディジタル署名を行うシステムにおいて、平文署名の一部としてメッセージを記入する一般的情報処理手段を含むことを特徴とする。

【０００６】本願の請求項６の電子文書署名方法は、センターと複数のメンバーがループ状にネットワークを構成して、電子文書（文書、図面、画像等）を回覧するシステムにおいて、制御プログラムを内蔵するメモリと、電子文書を作成する一般的情報処理手段と、電子文書を表示する表示部と、一方向性関数値Ｈ（Ｍ）を計算する手段と、情報部分を暗号化する手段と、復号化する手段と、ファイルを送信、転送する手段と、ファイル受信手段と、ファイル保存手段とを具備する電子文書署名装置において、文書発信者（あるいはセンター）は文書の送信の際には下記（１）ないし（７）の手順を含み、各メンバーは、下記（８）ないし（１４）の手順を含み、さらに、文書発信者（あるいはセンター）は文書の受信の際には下記（１５）ないし（１９）の手順を含むことを特徴とする。

文書発信者（あるいはセンター）の文書発信操作。

（１）通信文（文書、図面、画像等）を作成する手順。

（２）一方向性関数値Ｈ（Ｍ）を計算し、表示モードとして、発信元（センター）　　署名箇所にその計算値を記入（表示）する手順。

（３）さらに、発信元（センター）署名箇所に、発信元所属氏名（あるいはコード）、文書番号、月日時刻、メッセージを記入（表示）する手順。

（４）表示モードＨ（Ｍ）、発信元所属氏名（あるいはコード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化してバイナリディジタル署名を作成する手順。

（５）バイナリディジタル署名を表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する手順。

7

（6）次のメンバーへ転送する手順。
（7）ファイルを保存する手順。
【0007】各メンバーの操作。
（8）表示モードディジタル署名付通信文を受信する手順。
（9）表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する手順。
（10）平文署名を確認し、さらに、H（M）を再計算して文書に変更の無いことを確認する手順。
（11）自己の署名箇所にH（M）、所属氏名（あるいはコード）、文書番号、月日時刻、メッセージを記入（表示）し、平文署名を作成する手順。
（12）自己の秘密鍵で平文署名を暗号化して、バイナリディジタル署名とし、さらに表示モードディジタル署名に変換して自己の署名箇所に記入（表示）あるいはアペンドする手順。
（13）次のメンバーに転送する手順。
（14）ファイルを保存する手順。
文書発信者（あるいはセンター）の文書受信操作。
（15）表示モードディジタル署名付通信文を受信する手順。
（16）発信元（センター）および全メンバーの表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する手順。
（17）発信元（センター）および全メンバーの平文署名を確認し、H（M）を再計算し、文書に変更のないことを確認する手順。
（18）ファイルを保存する手順。
（19）全メンバーのディジタル署名付通信文を電子掲示板へ掲示（全メンバーに同報）する手順。
【0008】本願の請求項7の電子文書署名方法は、文書発信者（あるいはセンター）と複数のメンバーがスター状にネットワークを構成して、電子文書（文書、図面、画像等）を回覧するシステムにおいて、制御プログラムを内蔵するメモリと、通信文すなわち電子文書を作成する情報処理手段と、電子文書を表示する表示部と、ファイルを送信、転送する手段と、ファイル受信手段と、ファイル保存手段とを具備する電子文書署名装置において、文書発信者（あるいはセンター）は文書の送信の際には下記（20）ないし（26）の手順を含み、各メンバーは、下記（27）ないし（33）の手順を含み、さらに、文書発信者（あるいはセンター）は文書の受信の際には下記（34）ないし（39）の手順とを含むことを特徴とする。
文書発信者（あるいはセンター）の文書送信操作。
（20）通信文（文書、図面、画像等）を作成する手順。
（21）通信文Mより一方向性関数値H（M）を求め、表示モードとし、発信元（センター）署名箇所に、記入（表示）する手順。

8

（22）さらに、発信元（センター）署名箇所に、発信元所属氏名（あるいはコード）、文書番号、月日時刻、メッセージを記入（表示）する手順。
（23）表示モードH（M）、発信元元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化して、バイナリディジタル署名を作成する手順。
【0009】（24）バイナリディジタル署名を表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する。
（25）表示モードディジタル署名付通信文を電子掲示板へ掲示（全メンバーへ同報）する手順。
（26）ファイルを保存する手順。
各メンバーの操作。
（27）発信元（センター）より表示モードディジタル署名付き通信文を受信する手順。
（28）表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で復号する手順。
（29）平文署名を確認し、H（M）を再計算して文書に変更の無いことを確認する手順。
（30）自己のディジタル署名ファイルに表示モードH（M）、所属氏名、文書番号、月日時刻、メッセージを記入（表示）して平文署名を作成する手順。
（31）自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに、表示モードディジタル署名に変換する手順。
（32）自己の表示モードディジタル署名をセンターに送信する手順。
（33）ファイルを保存する手順。
【0010】文書発信者（あるいはセンター）の文書受信操作。
（34）各メンバーのディジタル署名を受信する手順。
（35）各メンバーのディジタル署名をそれぞれの公開鍵で復号して平文署名を得る手順。
（36）各メンバーの署名内容を確認する手順。
（37）通信文に暗号化された全メンバーの表示モードディジタル署名を付加する手順。
（38）ファイルを保存する手順。
（39）文書発信者（あるいはセンター）と全メンバーの表示モードディジタル署名付通信文を電子掲示板へ掲示（同報）する手順。
【0011】本願の請求項8の電子文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、通信文の属性を書換え禁止とする手段を含むことを特徴とする。本願の請求項9の電子文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、表示モードディジタル署名付通信文を用紙に印刷する印刷手段を含むことを特徴とする。本願の請求項10の電子文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシス

9

テムにおいて、印刷された表示モードディジタル署名付通信文の表示モードディジタル署名をスキャナなどでメモリに入力し表示部上に表示する手段と、前記表示モードディジタル署名をバイナリディジタル署名に変換し、さらに、平文署名に復号する復号化手段とを含むことを特徴とする。

【0012】

【作用】本願の電子文書署名方法および装置によれば、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、自己の平文署名として、通信文から計算される一方向性関数値H（M）、所属氏名（コード）、文書番号、月日時刻、メッセージを書き込み、秘密鍵で暗号化し、ディジタル署名として記入する。暗号化されたバイナリディジタル署名は表示モードディジタル署名に変換される。また、全メンバーのディジタル署名を公開鍵で復号化し、一方向性関数値H（M）を再計算し文書に変更の無いことを確認し、所属氏名、文書番号、月日時刻、メッセージを検査する。また、ディジタル署名付通信文が電子掲示板に表示され、全メンバーに同報される。

【0013】

【実施例】本発明の基本的発想は、実際に行われている回覧文書あるいは契約文書等の用紙上の文書の印鑑による認証を、可能な限りそのまま電子文書に適用しようとするものである。以下本発明をその実施例を示す図面に基づき詳述する。第1図は本発明の一実施例に係る電子文書署名装置の機能的構成を示すブロック図である。第2図はループ状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートであり、第3図はその通信文とディジタル署名例である。第4図はスター状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートであり、第5図はその通信文とディジタル署名例である。

【0014】第1図は電子文書（文書、図面、画像等）に1名以上のメンバーがディジタル署名を行うシステムにおいて、有効なディジタル署名を提供する電子文書署名装置の機能的構成を示すブロック図である。まず、制御部 1はマイクロプロセッサからなり、メモリ 3に書き込まれている制御プログラムにより後述するデータ処理を行う。以下この処理機能を有する仮想的ブロック図を想定して説明する。一般的情報処理手段 4は電子文書を作成し、それを表示部 2に表示する。ついで、一方向性関数H（M）計算手段 5は通信文（M）より、一方向性関数値H（M）を計算する。一般的情報処理手段 4は、平文の署名として、H（M）、所属氏名、文書番号、月日時刻、メッセージを書き込む。つぎに、ディジタル署名を作成するために情報部分選択手段 6で、平文を選択し、暗号化手段 7で、秘密鍵（公開鍵方式の復号鍵等）を用いて、H（M）、所属氏名、文書番号、月日時刻、メッセージを暗号化する。そして、バイナリー表示モード変換手段 9で、バイナリモードの暗号化されたディジタル署名を表示モードディジタル署名に変換して、画面等の表示部上で確認する。つぎに、ファイル送信、転送する手段 13でファイルを送信・転送し、ファイル保存手段 15でファイルを保存する。ファイル受信手段 14で電子文書を受信した際には、画面表示モードーバイナリ変換手段 10で、表示モードディジタル署名をバイナリディジタル署名に変換し、復号化手段8でディジタル署名を公開鍵（公開鍵方式では暗号鍵）で復号し、H（M）を再計算して署名内容を確認する。センターでは、電子掲示板に掲示する手段 12で通信文と全メンバーのディジタル署名とを電子掲示板に掲示（同報）する。ディジタル署名アペンド手段 11は通信文にディジタル署名をアペンドする。なお、平文署名を作成する際、画面表示するため一方向性関数値H（M）をバイナリー表示モード変換手段 9で表示モードに変換する。説明が複雑になるので、以下では、H（M）についてのこの処理は省略する。

10

【0015】以下に述べる発明を実施する際には、第1図の機能的手段のうちで必要なもののみを使用する。また、以下の説明および図面において、「画面表示」と単に「表示」は同じ意味で用いており、「画面を含めたいろいろな表示手段への表示」を意味する。本願の請求項1の電子文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、一般的情報処理手段 4によって、電子文書内に平文署名を記入し、情報部分選択手段 6で平文署名を選択する。選択した平文署名を秘密鍵を用いて暗号化手段 7で暗号化しディジタル署名を作成する。暗号化されたディジタル署名は情報部分選択手段 6によって選択され、公開鍵を用いて復号化手段 8によって、平文署名に復号される。本願の請求項2の電子文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、電子文書とは別ファイルに一般的情報処理手段 4で平文署名を記入し、その平文署名を秘密鍵を用いて暗号化手段 7で暗号化し、ディジタル署名を作成する。暗号化されたディジタル署名はディジタル署名アペンド手段 11で、電子文書にアペンドされる。

【0016】本願の請求項3の電子署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、バイナリディジタル署名をバイナリー表示モード変換手段 9によって、画面等の表示部上に表示するため表示モードディジタル署名に変換する。また、表示モードーバイナリ変換手段 10は、表示モードディジタル署名をバイナリディジタル署名に変換する。本願の請求項4の電子文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、一般的情報処理手段 4は、ディジタル署名として一方向性関数値H（M）、所属氏名または所属氏名を表すもの、文書番号、月日時刻を記入する。本願の請求項5の電子

文書署名装置は、電子文書に1名以上のメンバーがディジタル署名を行うシステムにおいて、一般的情報処理手段 4は、平文署名の一部としてメッセージを記入する。

【0017】次に、より具体的な実施例を示す。さて、ネットワークの構成には色々なものがあるが、原理的には、第6図ネットワークの論理的構成例に示すように（a）ループ状ネットワーク構成と（b）スター状ネットワーク構成に分けられる。つぎに、各々のネットワークにおける第1図の電子文書署名装置の動作例を第2図、第3図、第4図、第5図に基づき説明する。なお、第2図、第4図に示すフローチャートの説明中、N1、N2、・・・は処理手順（ステップ）を示す。本願の請求項6の電子文書署名方法の実施例について詳述する。第6図（a）のようにセンターと複数のメンバーが、ループ状にネットワークを構成して、電子文書（文書、図面、画像等）を回覧するシステムにおける動作について第2図、第3図を用いて述べる。メンバーから文書の発信が可能であるが、いま、センターから文書を発信したとする。

【0018】センターの文書送信操作は第2図（a）にしたがって次のようになる。N1で一般的情報処理手段 4によって通信文（文書、図面、画像等）を作成し、N2で一方向性関数H（M）計算手段 5によって一方向性関数値H（M）を計算し、バイナリー表示モード変換手段 9によって、表示モードにして、発信元（センター）署名箇所にその計算値を記入（表示）する。N3で一般的情報処理手段 4によって、発信元所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）する。N4で表示モードH（M）、発信元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化手段 7で暗号化して、バイナリディジタル署名を作成する。N5でバイナリー表示モード変換手段 9によって、バイナリディジタル署名を表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する。そして、N6でファイル送信、転送手段 13によって、次のメンバーへ転送する。N7でファイル保存手段 15によって、ファイルを保存する。

【0019】つぎに、各メンバーの操作は第2図（b）のようになる。N8でファイル受信手段 14によって画面表示モードディジタル署名付通信文を受信する。N9で表示モードーバイナリ変換手段 10によって、画面表示モードディジタルをバイナリディジタル署名に変換し、復号化手段 8によって、バイナリディジタル署名を公開鍵（公開鍵方式では暗号鍵）で復号する。N10で平文署名を確認し、一方向性関数H（M）計算手段 5でH（M）を再計算し、文書に変更の無いことを確認する。N11で一般的情報処理手段 4によって、自己の署名箇所にH（M）、所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）し平文署名を作成する。さらに、N12で暗号化手段 7によって、秘密鍵（公開鍵方式の復号鍵等）で平文署名を暗号化して、自己のバイナリディジタル署名を作成する。そして、バイナリー表示モード変換手段 9によって、画面表示ディジタル署名に変換して、自己の署名箇所に記入（表示）、あるいは、ディジタル署名アペンド手段 11によって、電子文書にディジタル署名をアペンドする。N13でファイル送信、転送する手段 13によって、次のメンバーに転送する。N14でファイル保存手段 15によって、ファイルを保存する。

【0020】センターの文書受信操作は第2図（c）のようになる。N15でファイル受信手段 14によって、通信文を受信する。N16で発信元（センター）および全メンバーの表示モードディジタル署名を表示モードーバイナリ変換手段 10によってバイナリディジタル署名に変換し、復号化手段 8によって、発信元（センター）の公開鍵（公開鍵方式では暗号鍵）で自己の署名を平文署名に復号する。N17で発信元（センター）および全メンバーの平文署名を確認し、一方向性関数H（M）計算手段 5によって、H（M）を再計算し、文書に変更のないことを確認する。N18でファイル保存手段 15によって、ファイルを保存する。N19で必要ならば、センターと全メンバーの表示モードディジタル署名付通信文を電子掲示板に掲示する手段 11によって電子掲示板に掲示するか、あるいは全メンバーに同報する。

【0021】第3図にループ状ネットワークを構成したときの同電子文書署名装置によって作成される通信文とディジタル署名の一例を示す。平文署名付通信文 20内に通信文 21と、ディジタル署名欄 22が用意されている。署名欄にセンターおよびメンバーは平文署名を記入する。各メンバーの署名欄に対して図のようにそれぞれ異なる句切り記号を用いているので、それによって署名部分を選択し、それぞれの暗号鍵で、部分的な暗号および復号を行う。句切り記号の代わりに、署名欄を座標あるいは変数で表しそれを基に署名欄を部分暗号してもよい。表示モードディジタル署名付通信文 30は通信文 31と、表示モードディジタル署名 32からなる。　なお、回覧すべき者、契約者等の署名者は通信文に記入してあるか、署名欄が用意されている。本願の請求項7の電子文書署名方法の実施例について詳述する。第6図（b）のようにセンターと複数のメンバーが、スター状にネットワークを構成して、電子文書（文書、図面、画像等）を回覧するシステムにおける動作について第4図、第5図を用いて述べる。センターが文書を電子掲示板に掲示あるいは同報し、各メンバーはディジタル署名のみセンターに送信する。なお、第1図の機能的ブロック図との関係はループ状ネットワークの場合と同様なので、以下の説明では省略する。

【0022】まず、センターの文書送信操作は第4図（a）にしたがって次のようになる。N20で通信文

（文書、図面、画像等）を作成する。Ｎ２１で一方向性関数値Ｈ（Ｍ）を計算し画面表示モードとし、、発信元（センター）署名箇所にその計算値を記入（表示）する。Ｎ２２で発信元（センター）署名箇所に発信元所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）する。Ｎ２３で、画面表示モードＨ（Ｍ）、発信元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化して、バイナリディジタル署名を作成する。Ｎ２４でバイナリディジタル署名を画面表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する。Ｎ２５で、画面表示モードディジタル署名付通信文を電子掲示板へ掲示あるいは全メンバーへ同報する。（必要ならば、メンバーにアクセス権を設定する。）Ｎ２６でファイルを保存する。

【００２３】各メンバーの操作は第４図（ｂ）のようになる。Ｎ２７で発信元（センター）より表示モードディジタル署名付通信文受信し、Ｎ２８で表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する。Ｎ２９で 平文署名を確認し、Ｈ（Ｍ）を再計算して文書に変更の無いことを確認する。Ｎ３０で自己のディジタル署名ファイルに表示モードＨ（Ｍ）、所属氏名（コード）、文書番号、月日時刻、メッセージを記入し、平文署名を作成する。Ｎ３１で、自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに表示モードディジタル署名に変換する。Ｎ３２で自己の表示モードディジタル署名をセンターへ送信する。Ｎ３３でファイルを保存する。 センターの文書受信操作は第４図（ｃ）のようになる。Ｎ３４で各メンバーの表示モードディジタル署名を受信する。Ｎ３５で各メンバーの表示モードディジタル署名をバイナリディジタル署名に変換し、さらに、それぞれの公開鍵で復号して平文署名を得る。Ｎ３６で各メンバーの署名の内容を確認する。Ｎ３７で通信文に暗号化された全メンバーの表示モードディジタル署名を付加する。Ｎ３８でファイルを保存する。Ｎ３９で必要ならば、センターと全メンバーの表示モードディジタル署名付通信文を電子掲示板に掲示（全メンバーへ同報）する。

【００２４】第５図にループ状ネットワークを構成したときの同電子文書署名装置によって作成される通信文とディジタル署名の一例を示す。表示モードディジタル署名付通信文 50が電子掲示板に掲示（同報）される。通信文 51と、表示モードディジタル署名欄 52とからなる。各メンバーは自己の表示モードディジタル署名 53, 54をセンターに送付する。センターでは元の電子文書に全メンバーの表示モードディジタル署名を付加して、再び電子掲示板に掲示（同報）する。なお、請求項８の発明は、通信文の属性を書換え禁止とし、一方向性関数値Ｈ（Ｍ）を用いず、ディジタル署名の内容を所属氏名（コード）、文書番号、月日時刻、メッセージとする電子文書署名方法および装置である。この発明は上記説明から容易に実施できるので詳細は省略する。また、請求項９の発明は、通信文と表示モードディジタル署名を用紙に印刷し、それを保存または他者に送り、その暗号部分を手入力、スキャナなどでメモリおよび表示部上に呼び込み復号手段で復号する電子文書署名方法および装置である。用紙上のディジタル署名は通常の印鑑と同様に扱うことができる。これも上記説明から容易に実施できるので詳細は省略する。なお、バイナリディジタル署名を表示部に表示しても良い、その時は表示されない部分ができる。また、画面の乱れには改行コードなどの変換などの処理が必要である。また、請求項７の発明の場合のように、メンバーがセンターに表示モードディジタル署名を送らないで、送信時に、バイナリディジタル署名に変換する方法も有効である。以上に述べた本発明の実施例は、ほんの一例に過ぎず、本発明を限定するものではない。いろいろなバリエーションがあり、それらも本発明に属する。

【００２５】

【発明の効果】以上説明したように、本発明の電子文書署名方法および装置は、電子文書に１名以上のメンバーが印鑑と同様に、署名部分を選択し、秘密の暗号鍵を用いてディジタル署名をすることが可能である。しかも、表示モードディジタル署名を使って、マン・マシン・インタフェイスに優れたディジタル署名システムが実現できる。

【図面の簡単な説明】

【図１】本発明の一実施例に係る電子文書署名装置の機能的構成を示すブロック図である。

【図２】ループ状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートである。（ａ）はセンター装置の文書発信フローチャート、（ｂ）はメンバー装置のフローチャート、（ｃ）はセンター装置の文書受信フローチャート。

【図３】ループ状ネットワークを構成したときの同電子文書署名装置によって作成される通信文とディジタル署名。

【図４】スター状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートである。（ａ）はセンター装置の文書発信フローチャート、（ｂ）はメンバー装置のフローチャート、（ｃ）はセンター装置の文書受信フローチャート。

【図５】スター状ネットワークを構成したときの同電子文書署名装置によって作成される通信文とディジタル署名である。

【図６】ネットワークの論理的構成例である。（ａ）はループ状ネットワーク構成、（ｂ）はスター状ネットワーク構成である。

【図７】ディジタル署名原理図である。

【符号の説明】

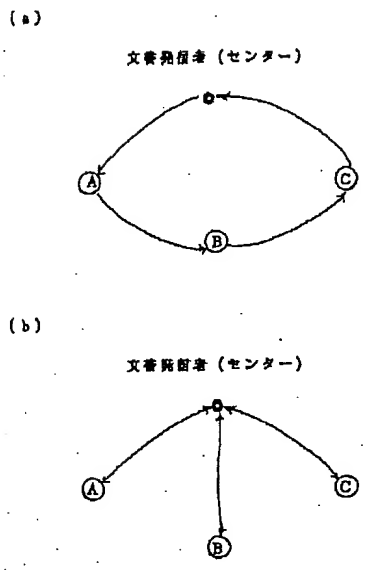
15

1　制御部
2　表示部
3　メモリ
4　一般的情報処理手段
5　一方向性関数Ｈ（Ｍ）計算手段
6　情報部分選択手段
7　暗号化手段
8　復号化手段
9　バイナリー表示モード変換手段
１０　表示モードーバイナリ変換手段
１１　ディジタル署名アペンド手段
１２　電子掲示板（同報）手段
１３　ファイル送信・転送手段
１４　ファイル受信手段
１５　ファイル保存手段

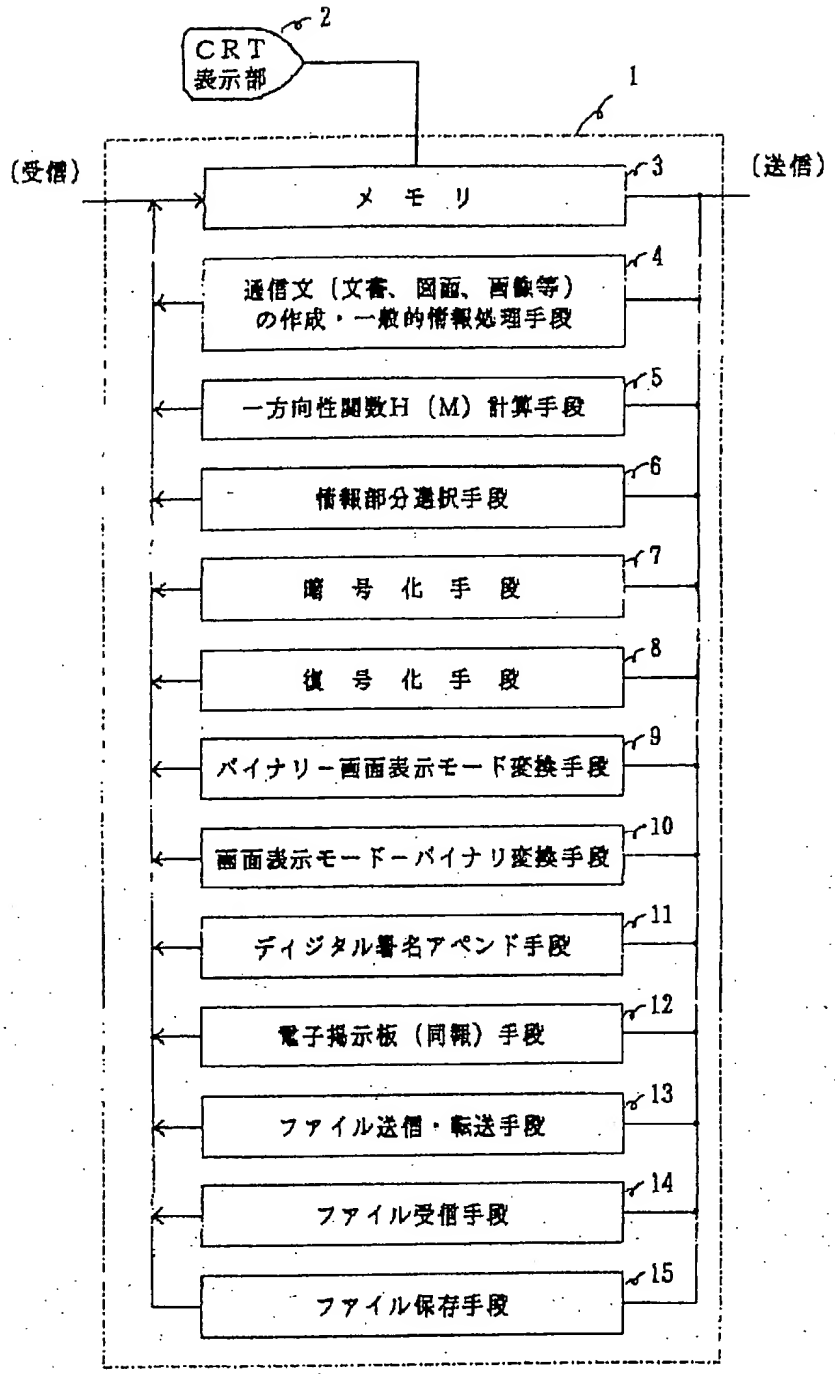
16

２０　平文署名付通信文
２１　通信文
２２　平文署名
３０　表示モードディジタル署名付通信文
３１　通信文
３２　表示モードディジタル署名
５０　表示モードディジタル署名付通信文
５１　通信文
５２　表示モードディジタル署名
５３　表示モードディジタル署名
５４　表示モードディジタル署名
１００　一方向性関数Ｈ（Ｍ）計算手段
１０１　暗号化手段
１０２　復号化手段

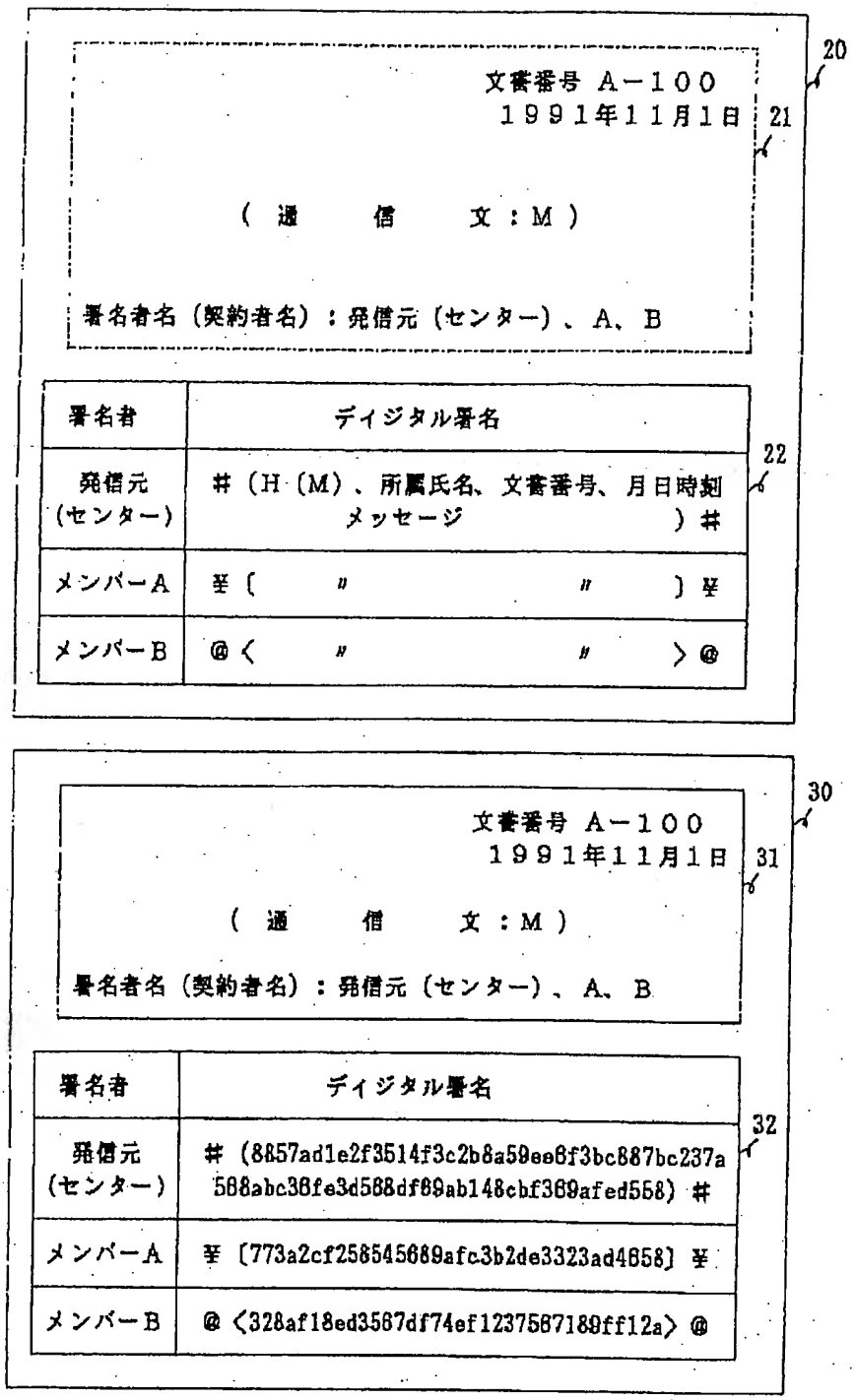
【図６】



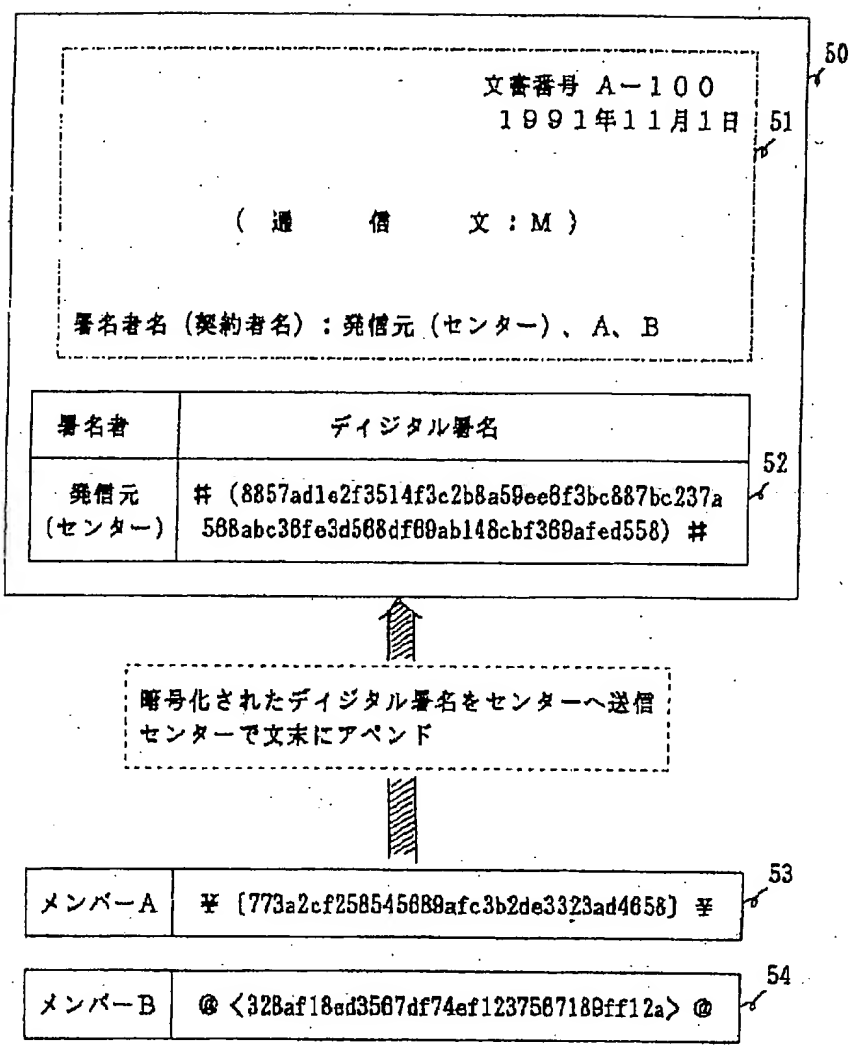
【図1】


CRT
表示部
2
1
(受信)
(送信)
メ モ リ
3
通信文（文書、図面、画像等）
の作成・一般的情報処理手段
4
一方向性関数H（M）計算手段
5
情報部分選択手段
6
暗 号 化 手 段
7
復 号 化 手 段
8
バイナリー画面表示モード変換手段
9
画面表示モードーバイナリ変換手段
10
ディジタル署名アペンド手段
11
電子掲示板（同報）手段
12
ファイル送信・転送手段
13
ファイル受信手段
14
ファイル保存手段
15

【図3】

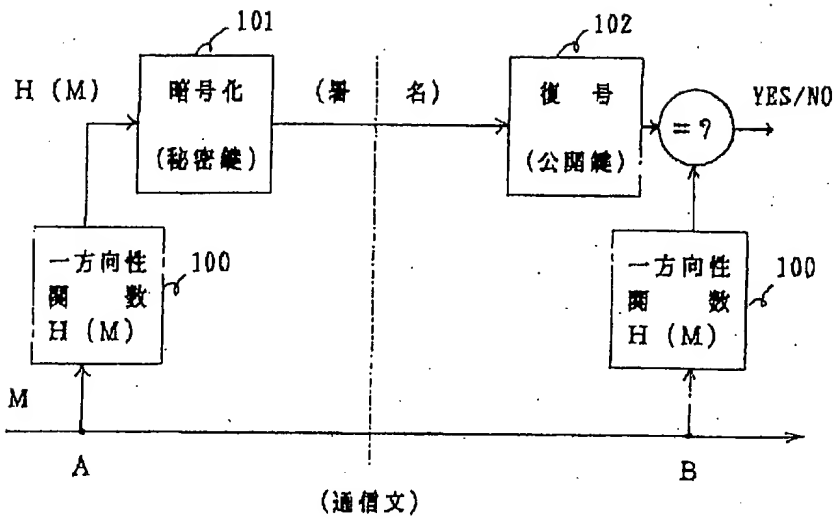

20
文書番号 A－100
1991年11月1日
21
（ 通 信 文：M ）
署名者名（契約者名）：発信元（センター）、A、B
署名者
ディジタル署名
発信元（センター）
＃（H（M）、所属氏名、文書番号、月日時刻 メッセージ ）＃
メンバーA
〒〔 〃 〃 〕〒
メンバーB
@〈 〃 〃 〉@
22
30
文書番号 A－100
1991年11月1日
31
（ 通 信 文：M ）
署名者名（契約者名）：発信元（センター）、A、B
署名者
ディジタル署名
発信元（センター）
＃（8857ad1e2f3514f3c2b8a59ee6f3bc887bc237a588abc36fe3d588df89ab148cbf369afed558）＃
メンバーA
〒〔773a2cf258545689afc3b2de3323ad4658〕〒
メンバーB
@〈328af18ed3567df74ef1237567189ff12a〉@
32

【図５】



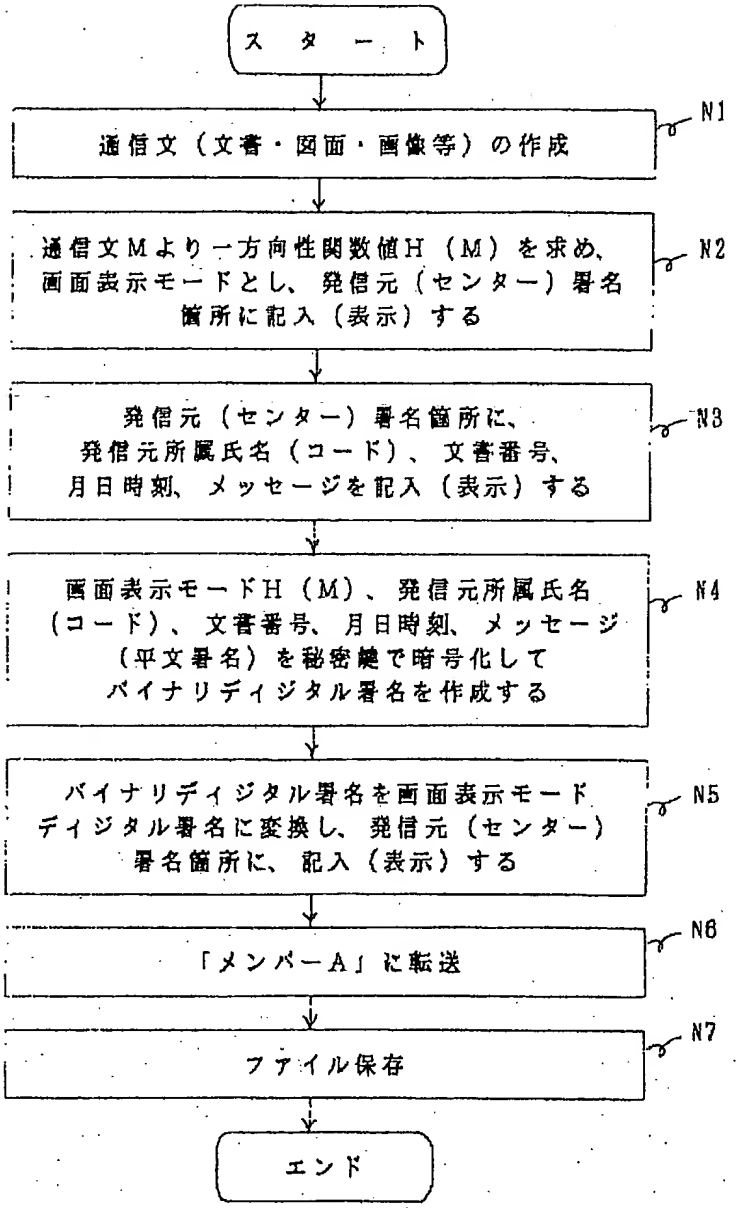
署名の内容：H（M）、所属氏名、文書番号、月日時刻、メッセージ

【図7】


101
102
H（M）
暗号化
（秘密鍵）
（署　名）
復　号
（公開鍵）
=?
YES/NO
一方向性
関　数
H（M）
100
一方向性
関　数
H（M）
100
M
A
B
（通信文）

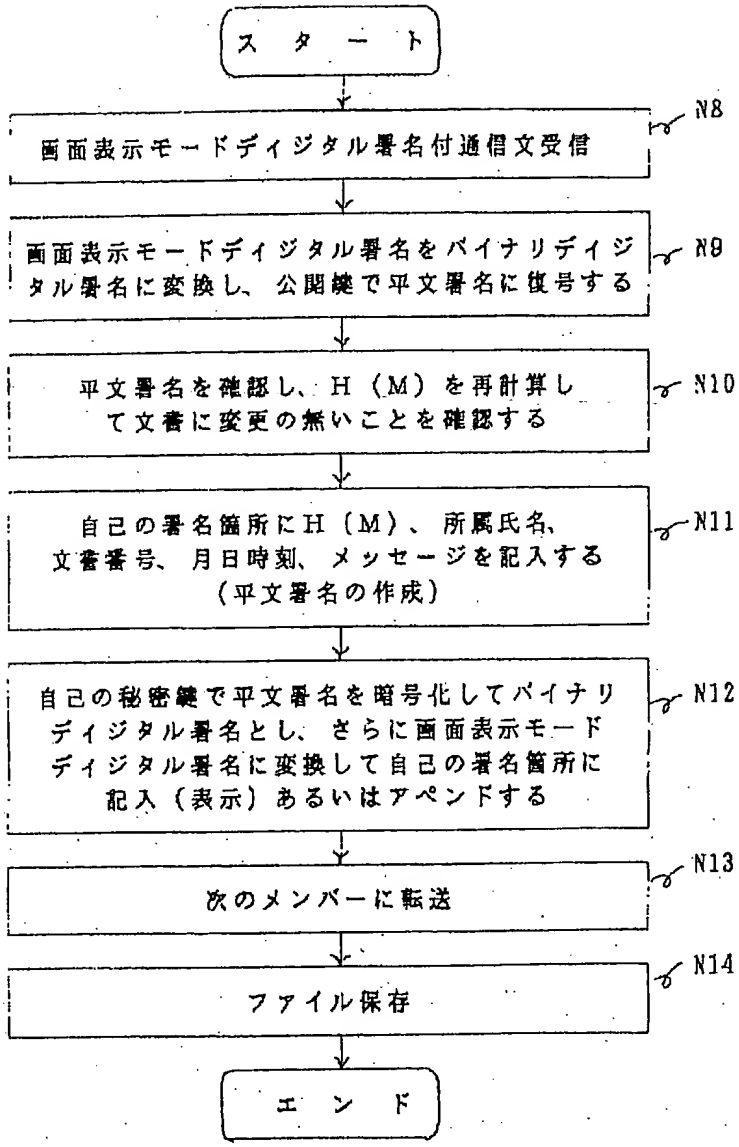
【図2】

（a）


スタート
通信文（文書・図面・画像等）の作成
N1
通信文Mより一方向性関数値H（M）を求め、画面表示モードとし、発信元（センター）署名箇所に記入（表示）する
N2
発信元（センター）署名箇所に、発信元所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）する
N3
画面表示モードH（M）、発信元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化してバイナリディジタル署名を作成する
N4
バイナリディジタル署名を画面表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する
N5
「メンバーA」に転送
N6
ファイル保存
N7
エンド

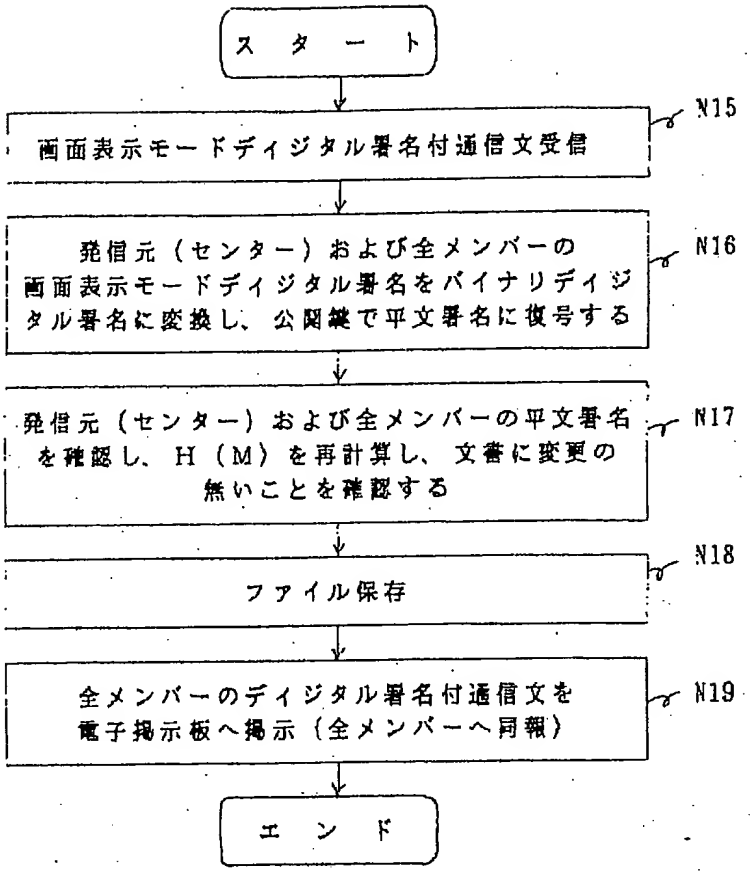
【図2】

(b)


スタート
画面表示モードディジタル署名付通信文受信
N8
画面表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する
N9
平文署名を確認し、H（M）を再計算して文書に変更の無いことを確認する
N10
自己の署名箇所にH（M）、所属氏名、文書番号、月日時刻、メッセージを記入する（平文署名の作成）
N11
自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに画面表示モードディジタル署名に変換して自己の署名箇所に記入（表示）あるいはアペンドする
N12
次のメンバーに転送
N13
ファイル保存
N14
エンド

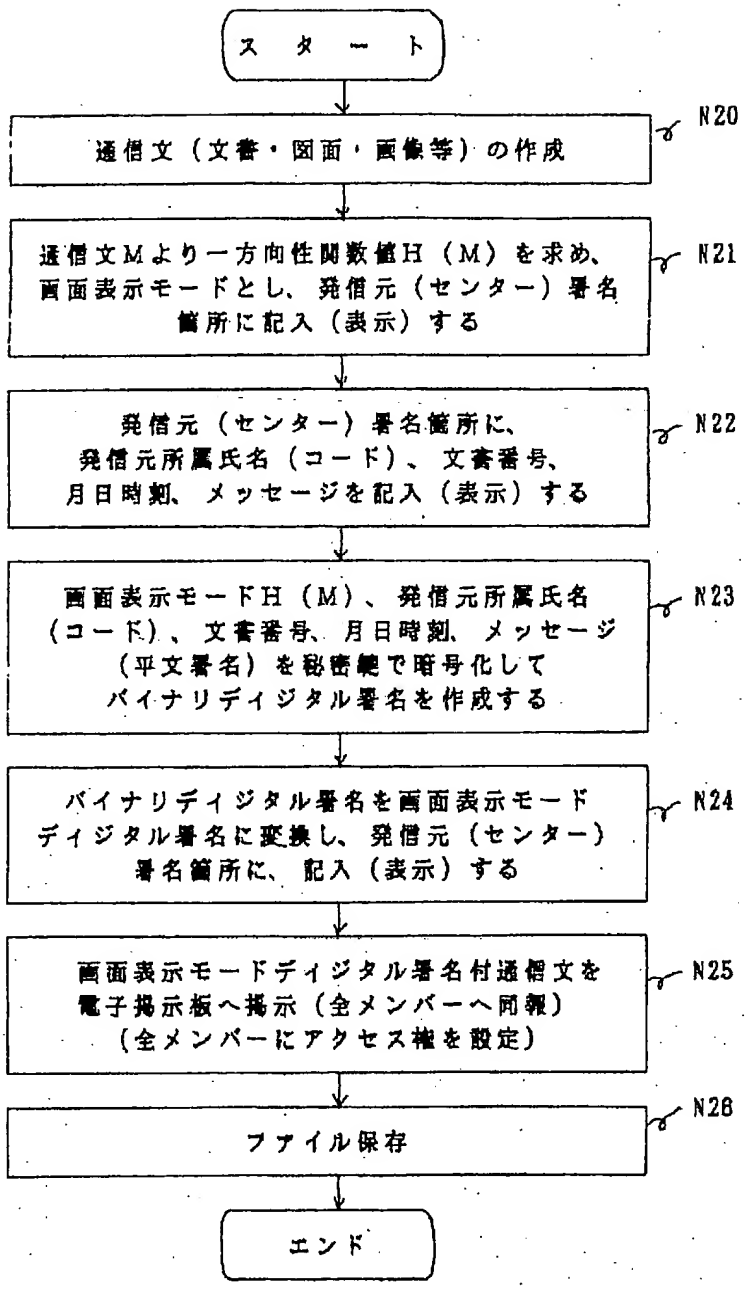
【図2】

（c）


スタート
画面表示モードディジタル署名付通信文受信
N15
発信元（センター）および全メンバーの画面表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する
N16
発信元（センター）および全メンバーの平文署名を確認し、H（M）を再計算し、文書に変更の無いことを確認する
N17
ファイル保存
N18
全メンバーのディジタル署名付通信文を電子掲示板へ掲示（全メンバーへ同報）
N19
エンド

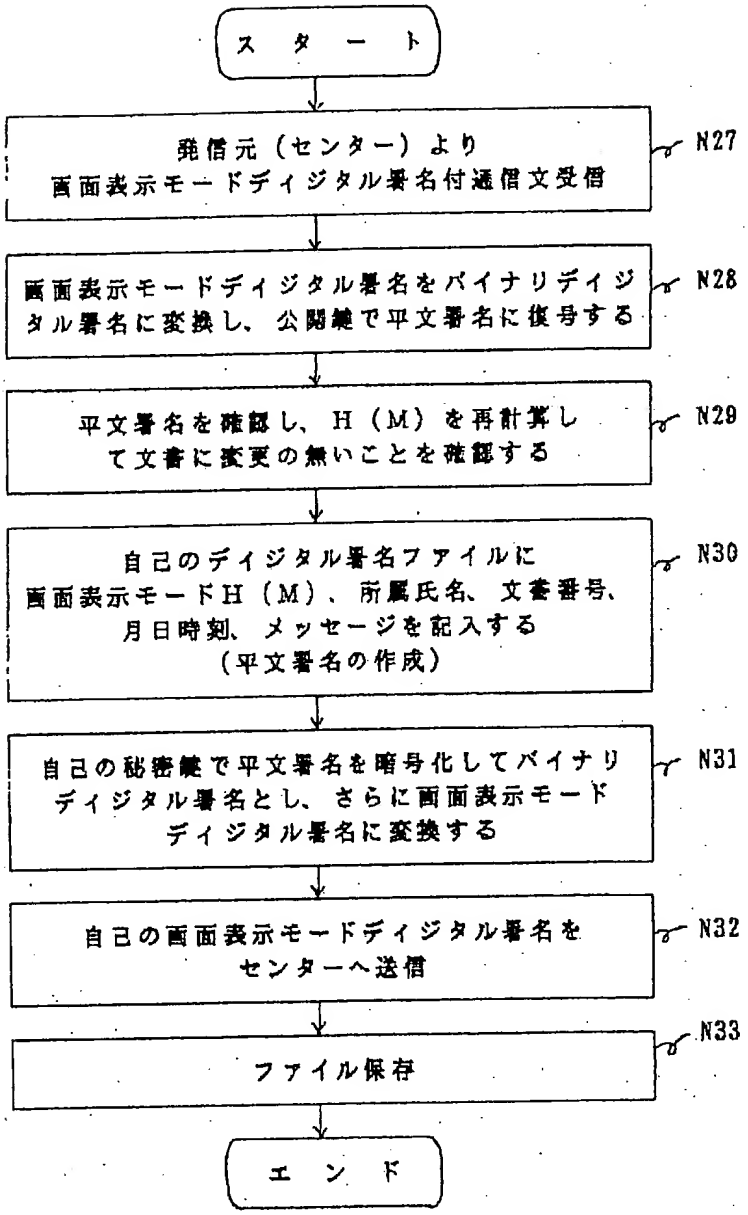
【図4】

（a）


スタート
通信文（文書・図面・画像等）の作成
N20
通信文Mより一方向性関数値H（M）を求め、画面表示モードとし、発信元（センター）署名箇所に記入（表示）する
N21
発信元（センター）署名箇所に、発信元所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）する
N22
画面表示モードH（M）、発信元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化してバイナリディジタル署名を作成する
N23
バイナリディジタル署名を画面表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する
N24
画面表示モードディジタル署名付通信文を電子掲示板へ掲示（全メンバーへ同報）（全メンバーにアクセス権を設定）
N25
ファイル保存
N26
エンド

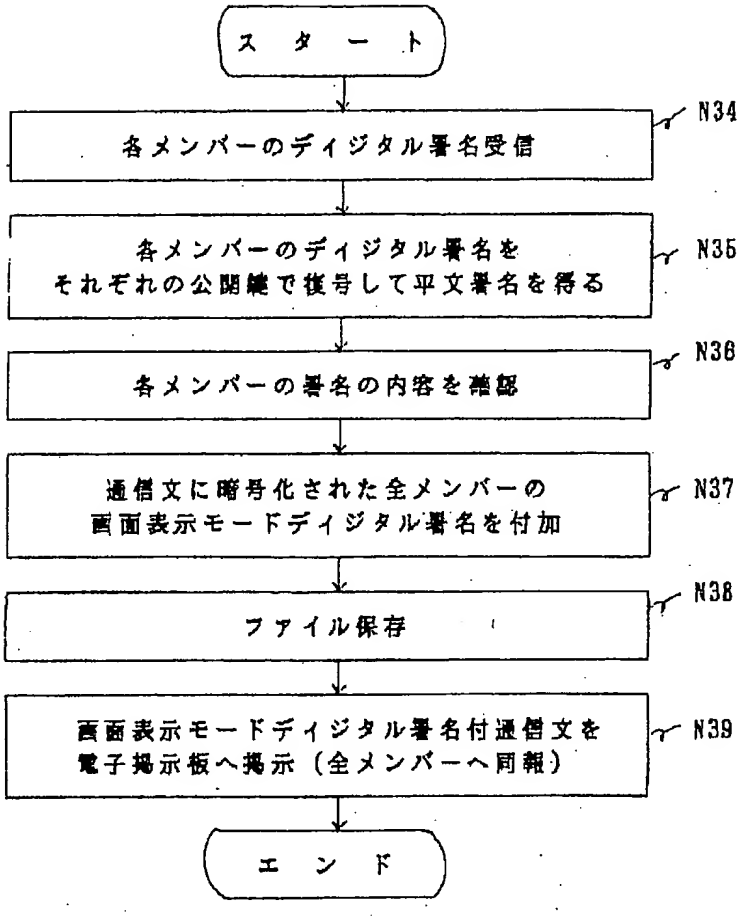
【図4】

(b)


スタート
発信元（センター）より
画面表示モードディジタル署名付通信文受信
N27
画面表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する
N28
平文署名を確認し、H（M）を再計算して文書に変更の無いことを確認する
N29
自己のディジタル署名ファイルに
画面表示モードH（M）、所属氏名、文書番号、
月日時刻、メッセージを記入する
（平文署名の作成）
N30
自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに画面表示モードディジタル署名に変換する
N31
自己の画面表示モードディジタル署名を
センターへ送信
N32
ファイル保存
N33
エンド

【図4】

（c）



【手続補正書】
【提出日】平成5年8月2日
【手続補正3】
【補正対象書類名】明細書
【補正対象項目名】図面の簡単な説明
【補正方法】変更
【補正内容】
【図面の簡単な説明】
【図1】本発明の一実施例に係る電子文書署名装置の機能的構成を示すブロック図である。
【図2】ループ状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートのうち、センター装置の文書発信フローチャート（a）である。
【図3】ループ状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートのうち、メンバー装置のフローチャート（b）である。
【図4】ループ状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートのうち、センター装置の文書受信フローチャート（c）である。
【図5】ループ状ネットワークを構成したときの同電子文書署名装置によって作成される通信文とディジタル署名。
【図6】スター状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートのうち、センター装置の文書発信フローチャート（a）である。
【図7】スター状ネットワークを構成したときの同電子文書署名装置の作動を示すフローチャートのうち、メンバー装置のフローチャート（b）である。
【図8】スター状ネットワークを構成したときの同電子

文書署名装置の作動を示すフローチャートのうち、センター装置の文書受信フローチャート（ｃ）である。

【図９】スター状ネットワークを構成したときの同電子文書署名装置によって作成される通信文とディジタル署名である。

【図１０】ネットワークの論理的構成例である。（ａ）はループ状ネットワーク構成、（ｂ）はスター状ネットワーク構成である。

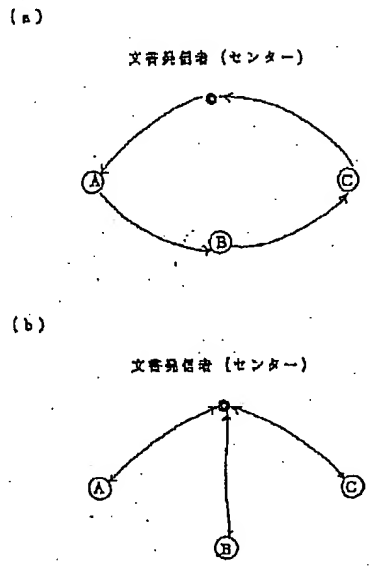
【図１１】ディジタル署名原理図である。

【符号の説明】

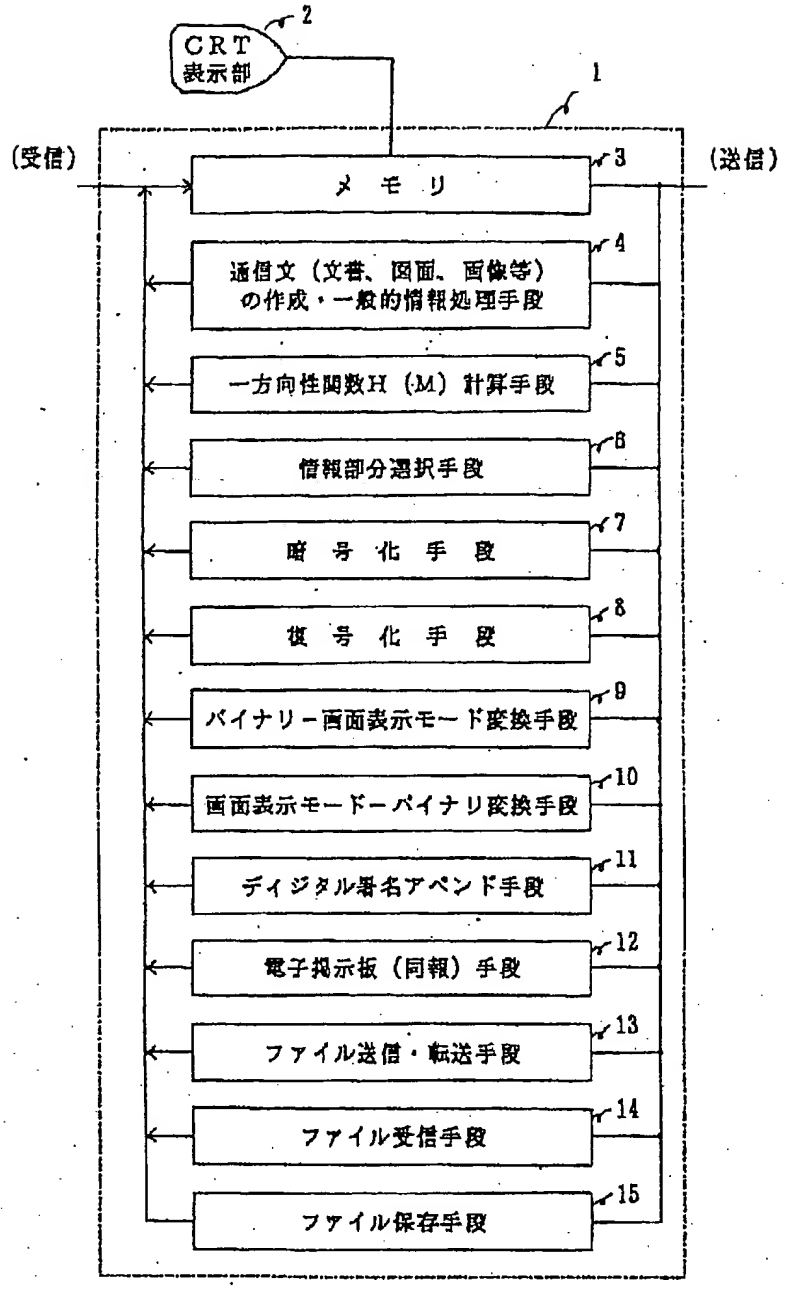
１　制御部
２　表示部
３　メモリ
４　一般的情報処理手段
５　一方向性関数Ｈ（Ｍ）計算手段
６　情報部分選択手段
７　暗号化手段
８　復号化手段
９　バイナリー表示モード変換手段
１０　表示モードーバイナリ変換手段
１１　ディジタル署名アペンド手段
１２　電子掲示板（同報）手段
１３　ファイル送信・転送手段
１４　ファイル受信手段
１５　ファイル保存手段
２０　平文署名付通信文
２１　通信文
２２　平文署名
３０　表示モードディジタル署名付通信文
３１　通信文
３２　表示モードデイジタル署名
５０　表示モードデイジタル署名付通信文
５１　通信文
５２　表示モードディジタル署名
５３　表示モードディジタル署名
５４　表示モードディジタル署名
１００　一方向性関数Ｈ（Ｍ）計算手段
１０１　暗号化手段
１０２　復号化手段

【手続補正４】
【補正対象書類名】図面
【補正対象項目名】全図
【補正方法】変更
【補正内容】

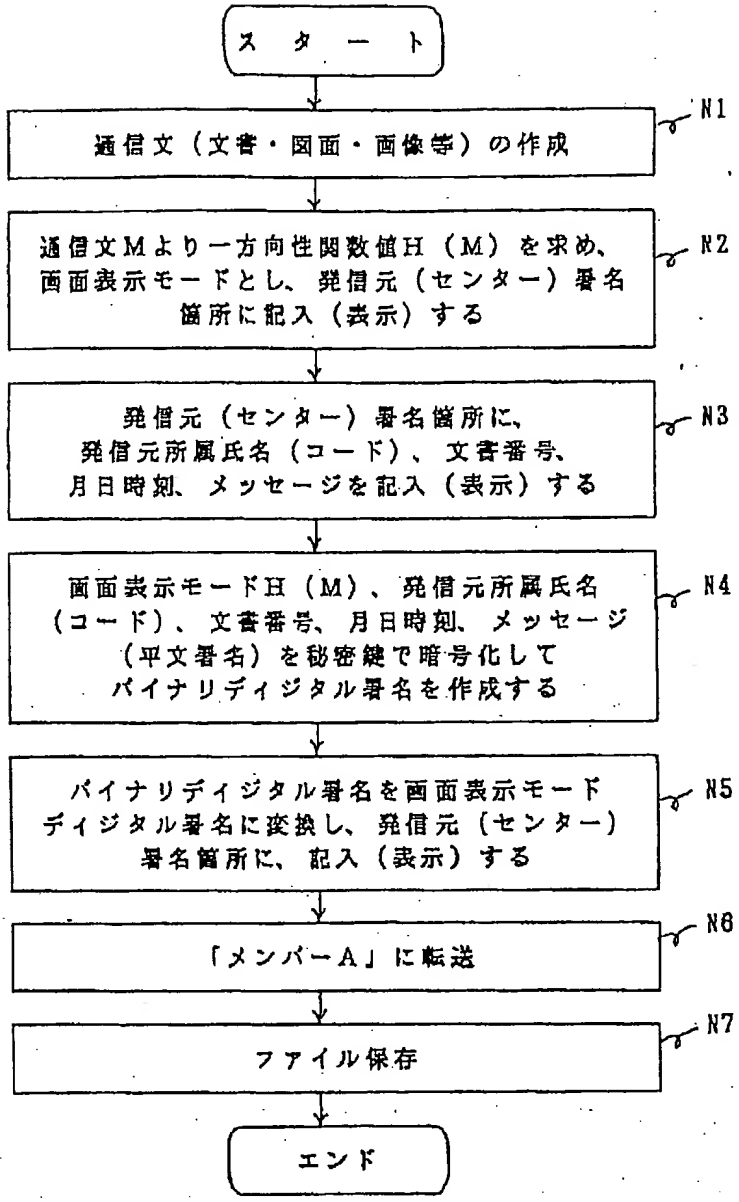
【図１０】



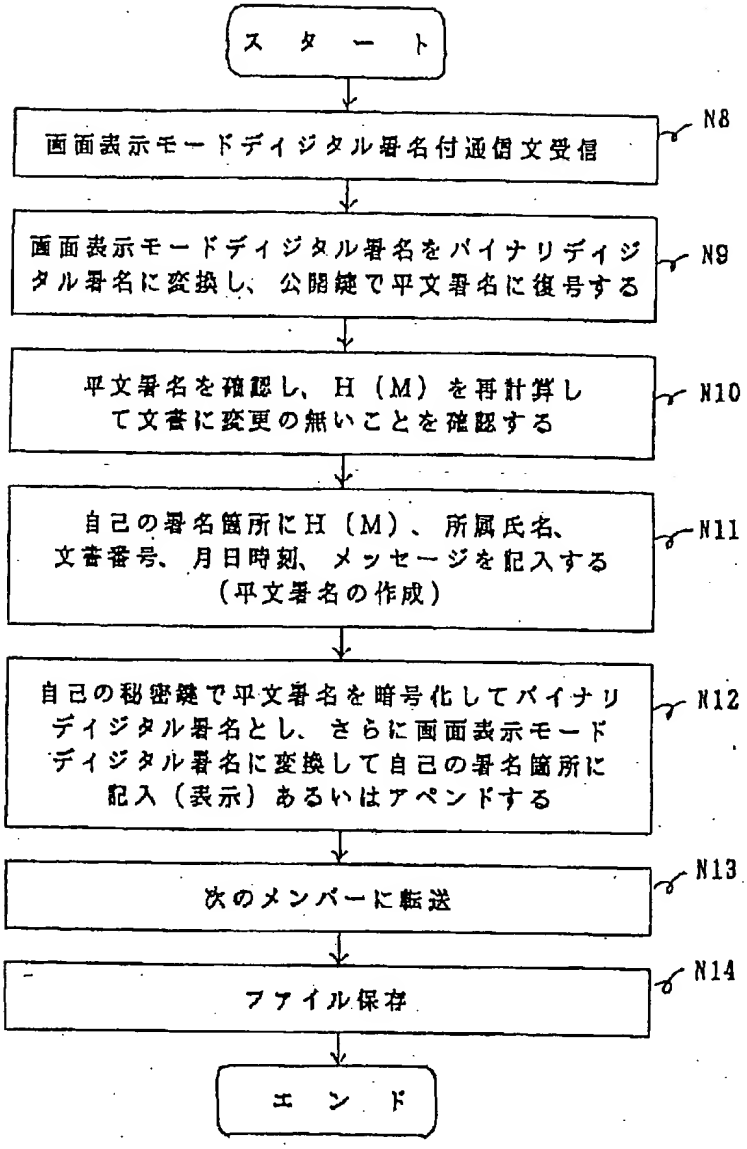
[図1]


CRT
表示部
2
1
(受信)
(送信)
メモリ
3
通信文（文書、図面、画像等）の作成・一般的情報処理手段
4
一方向性関数H（M）計算手段
5
情報部分選択手段
6
暗号化手段
7
復号化手段
8
バイナリー画面表示モード変換手段
9
画面表示モードーバイナリ変換手段
10
ディジタル署名アペンド手段
11
電子掲示板（同報）手段
12
ファイル送信・転送手段
13
ファイル受信手段
14
ファイル保存手段
15

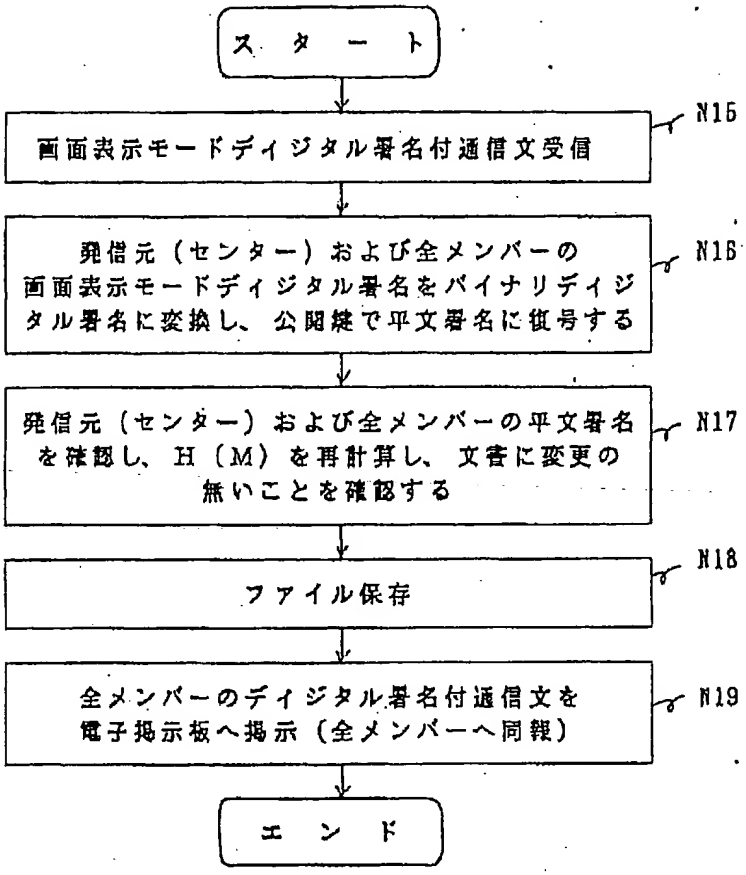
[図2]


スタート
通信文（文書・図面・画像等）の作成
N1
通信文Mより一方向性関数値H（M）を求め、画面表示モードとし、発信元（センター）署名箇所に記入（表示）する
N2
発信元（センター）署名箇所に、発信元所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）する
N3
画面表示モードH（M）、発信元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化してバイナリディジタル署名を作成する
N4
バイナリディジタル署名を画面表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する
N5
「メンバーA」に転送
N6
ファイル保存
N7
エンド

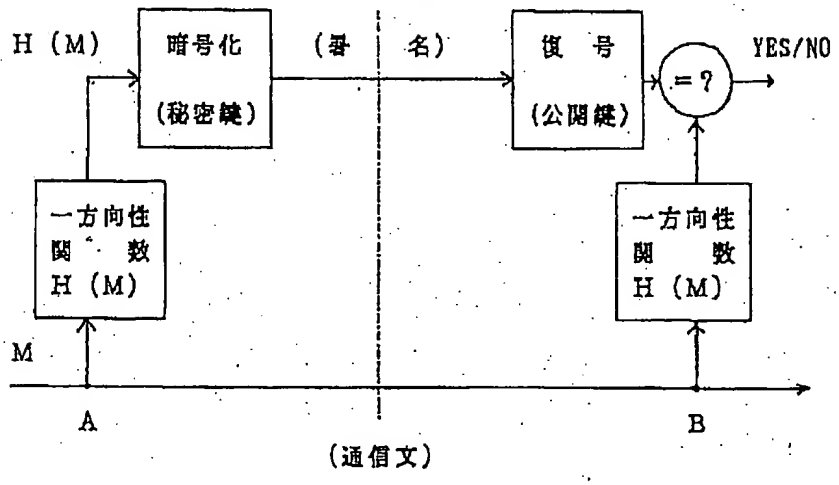
【図8】


スタート
画面表示モードディジタル署名付通信文受信
N8
画面表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する
N9
平文署名を確認し、H（M）を再計算して文書に変更の無いことを確認する
N10
自己の署名箇所にH（M）、所属氏名、文書番号、月日時刻、メッセージを記入する（平文署名の作成）
N11
自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに画面表示モードディジタル署名に変換して自己の署名箇所に記入（表示）あるいはアペンドする
N12
次のメンバーに転送
N13
ファイル保存
N14
エンド

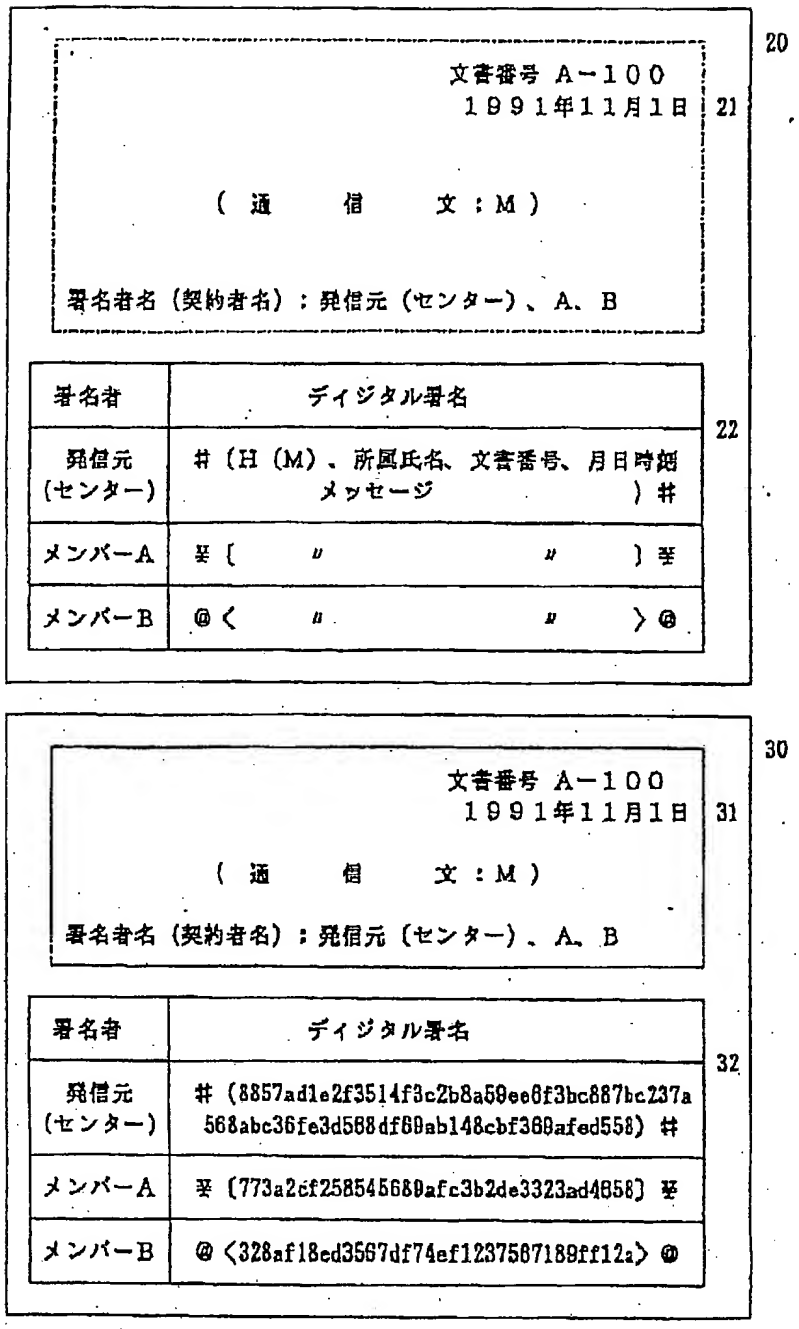
【図4】


スタート
画面表示モードディジタル署名付通信文受信
N15
発信元（センター）および全メンバーの画面表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する
N16
発信元（センター）および全メンバーの平文署名を確認し、H（M）を再計算し、文書に変更の無いことを確認する
N17
ファイル保存
N18
全メンバーのディジタル署名付通信文を電子掲示板へ掲示（全メンバーへ同報）
N19
エンド

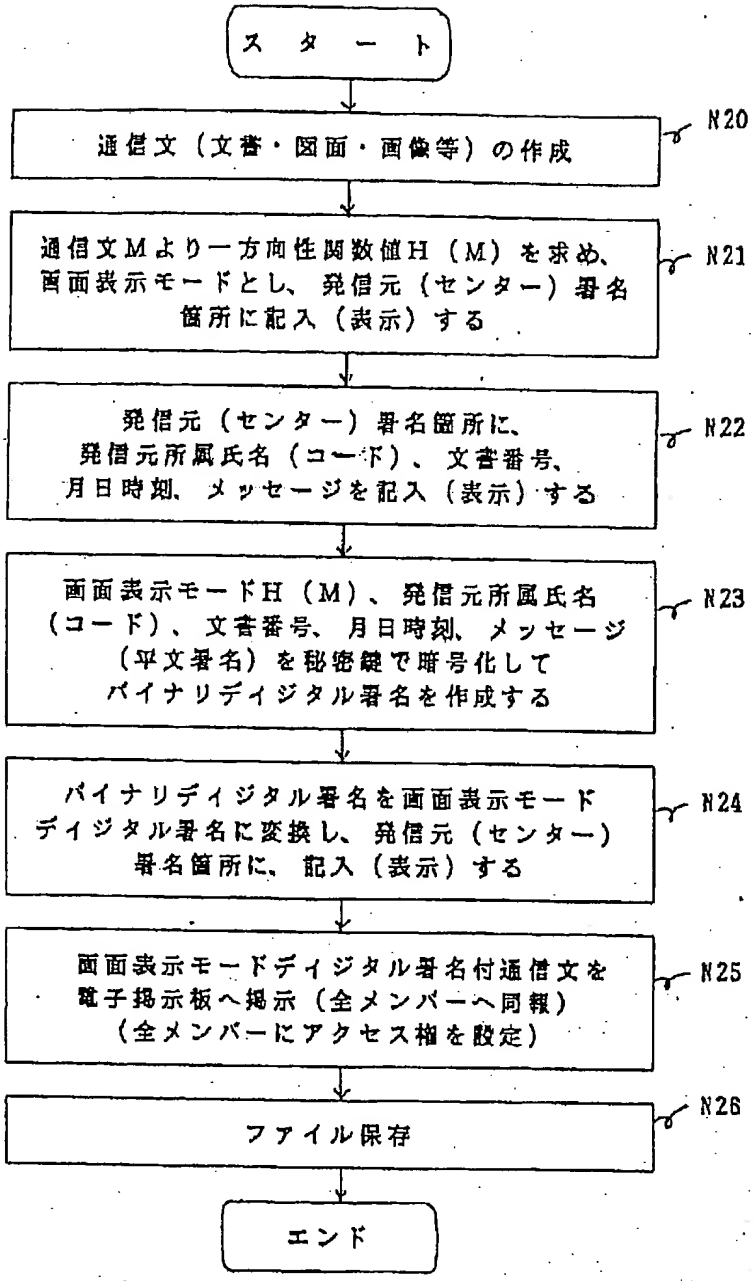
【図11】


H（M）
暗号化
（秘密鍵）
（署　名）
復　号
（公開鍵）
=？
YES/NO
一方向性関数 H（M）
一方向性関数 H（M）
M
A
B
（通信文）

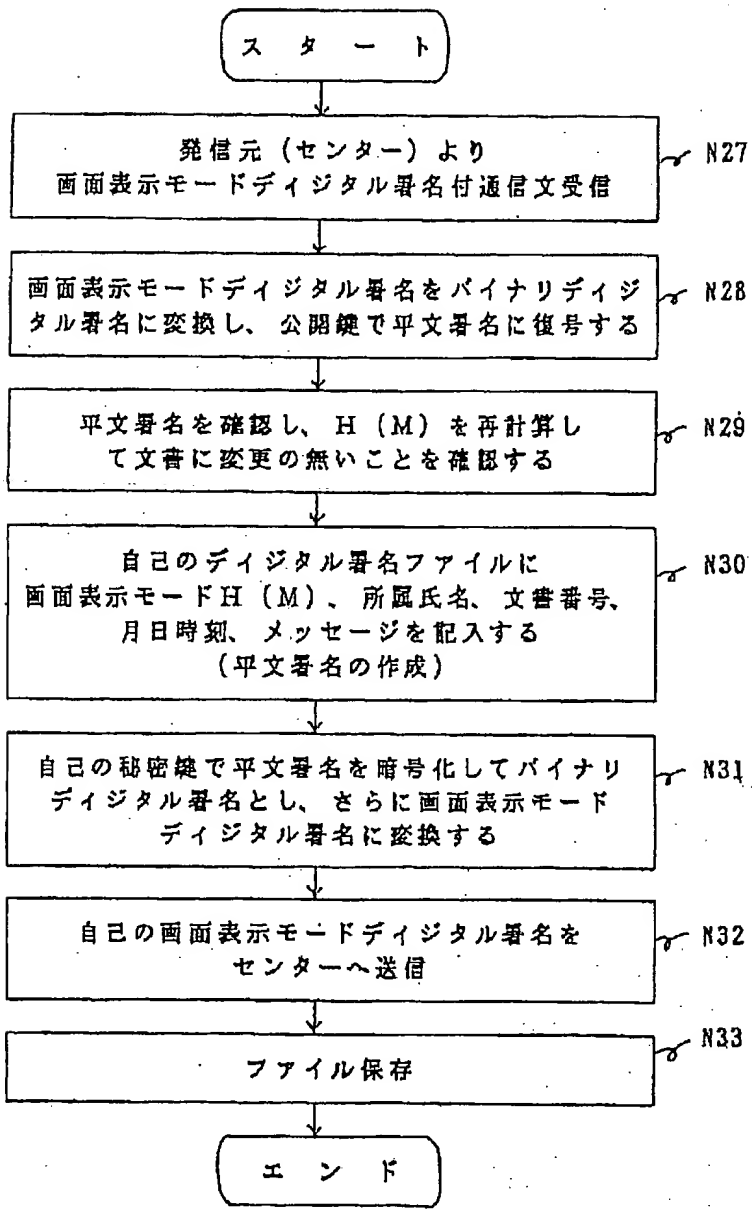
【図5】


20
文書番号 A－100
1991年11月1日
21
（通　　信　　文：M）
署名者名（契約者名）：発信元（センター）、A、B
署名者
ディジタル署名
発信元（センター）
＃（H（M）、所属氏名、文書番号、月日時刻メッセージ）＃
メンバーA
〒（　〃　〃　）〒
メンバーB
@〈　〃　〃　〉@
22
30
文書番号 A－100
1991年11月1日
31
（通　　信　　文：M）
署名者名（契約者名）：発信元（センター）、A、B
署名者
ディジタル署名
発信元（センター）
＃（8857ad1e2f3514f3c2b8a59ee6f3bc887bc237a568abc36fe3d568df69ab148cbf369afed558）＃
メンバーA
〒（773a2cf258545689afc3b2de3323ad4858）〒
メンバーB
@〈328af18ed3567df74ef1237567189ff12a〉@
32

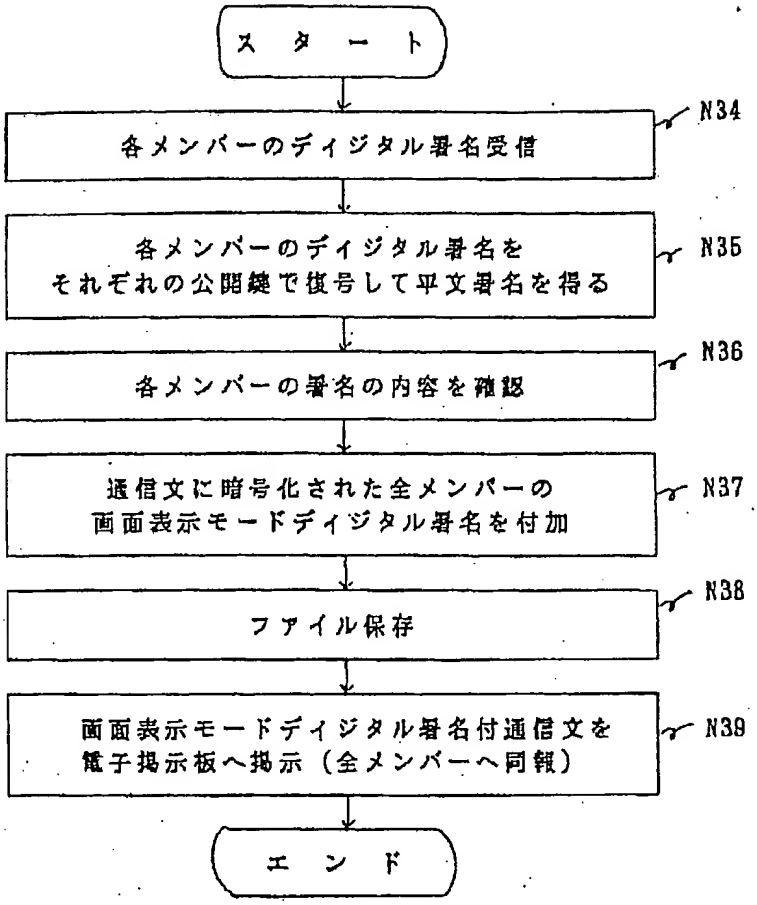
【図6】


スタート
通信文（文書・図面・画像等）の作成
N20
通信文Mより一方向性関数値H（M）を求め、画面表示モードとし、発信元（センター）署名箇所に記入（表示）する
N21
発信元（センター）署名箇所に、発信元所属氏名（コード）、文書番号、月日時刻、メッセージを記入（表示）する
N22
画面表示モードH（M）、発信元所属氏名（コード）、文書番号、月日時刻、メッセージ（平文署名）を秘密鍵で暗号化してバイナリディジタル署名を作成する
N23
バイナリディジタル署名を画面表示モードディジタル署名に変換し、発信元（センター）署名箇所に、記入（表示）する
N24
画面表示モードディジタル署名付通信文を電子掲示板へ掲示（全メンバーへ同報）（全メンバーにアクセス権を設定）
N25
ファイル保存
N26
エンド

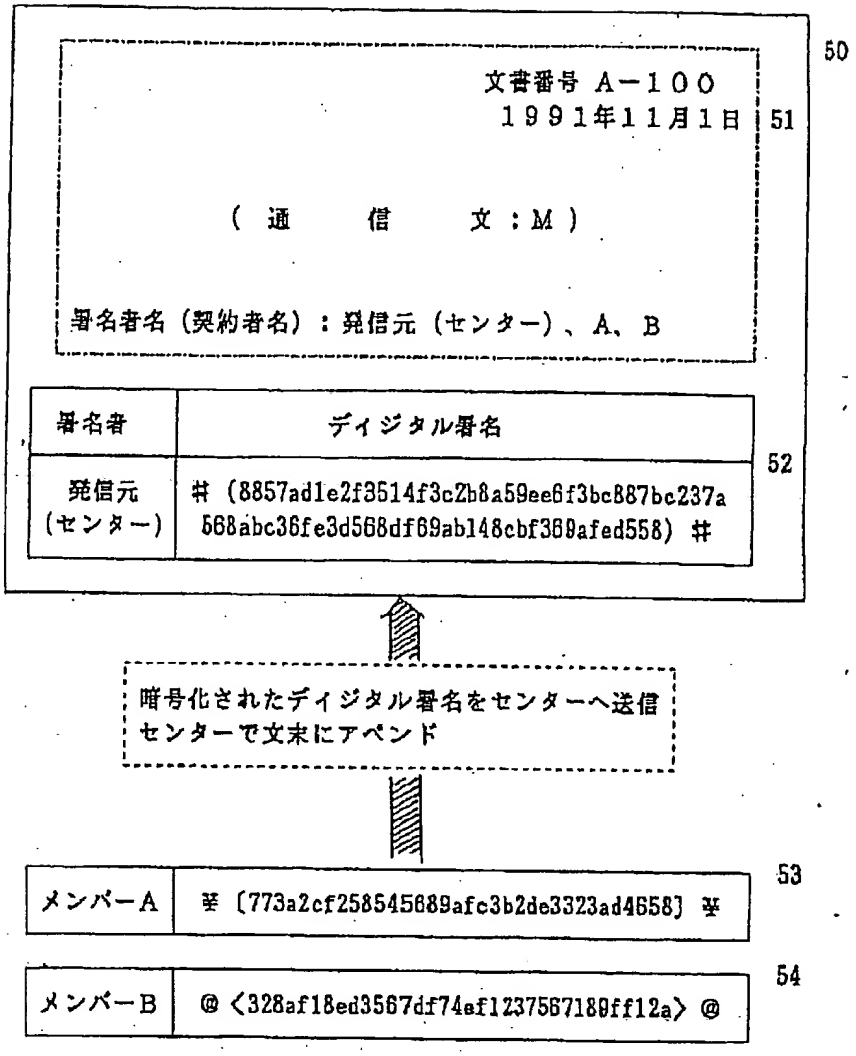
【図7】


スタート
発信元（センター）より
画面表示モードディジタル署名付通信文受信
N27
画面表示モードディジタル署名をバイナリディジタル署名に変換し、公開鍵で平文署名に復号する
N28
平文署名を確認し、H（M）を再計算して文書に変更の無いことを確認する
N29
自己のディジタル署名ファイルに
画面表示モードH（M）、所属氏名、文書番号、
月日時刻、メッセージを記入する
（平文署名の作成）
N30
自己の秘密鍵で平文署名を暗号化してバイナリディジタル署名とし、さらに画面表示モードディジタル署名に変換する
N31
自己の画面表示モードディジタル署名を
センターへ送信
N32
ファイル保存
N33
エンド

[図8]


スタート
各メンバーのディジタル署名受信
N34
各メンバーのディジタル署名を
それぞれの公開鍵で復号して平文署名を得る
N35
各メンバーの署名の内容を確認
N36
通信文に暗号化された全メンバーの
画面表示モードディジタル署名を付加
N37
ファイル保存
N38
画面表示モードディジタル署名付通信文を
電子掲示板へ掲示（全メンバーへ同報）
N39
エンド

【図9】



署名の内容：H（M）、所属氏名、文書番号、月日時刻、メッセージ

フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
H04L 9/14				
12/22				